MATHEMATICS 144
SET THEORY
FALL 2012 VERSION

Table of Contents

(iv + 210 pages)

PREFACE

This is a slightly modified set of notes from the most recent time I taught Mathematics 144, which was during the Fall 2006 Quarter. There are only a few minor revisions and insertions, with updated biographical information and links as needed. Since clickable Internet references appear frequently in the notes, I have also included my standard policy remarks about the use of such material.

The official main text for this course was the book on set theory in the Schaum's Outline Series by S. Lipschutz, but for several abstract or technical issues there are references to previously used course texts by P. Halmos and D. Goldrei (see page 1 for detailed information on all three of these books). The online directory for the 2006 course

http://math.ucr.edu/~res/math144/

also contains several files of exercises and solutions based upon the notes.

Most of the set – theoretic notation is extremely standard, and we shall also employ some frequently used conventions for using "blackboard bold letters" and other characters to denote familiar sets and number systems:

$\emptyset$	*empty set*
$\mathbb{N}$	*natural numbers = nonnegative integers*
$\mathbb{Z}$	*(signed) integers*
$\mathbb{Q}$	*rational numbers*
$\mathbb{R}$	*real numbers*
$\mathbb{C}$	*complex numbers*

Similarly, we shall use $\mathbb{R}^n$ to denote the usual analytic representation of ***Euclidean*** or ***Cartesian*** n **–** [*dimensional*] ***space*** in terms of coordinates $(x_1, \ldots, x_n)$, where the x_i's are all real numbers.

As in calculus, if **a** and **b** are real numbers or $\pm\infty$ with **a < b**, we define ***intervals*** as follows:

Notation	*Type of interval*	*Defining inequalties*
(a, b)	open	**a < x < b**
[a, b]	closed	**a ≤ x ≤ b**
(a, b]	half open	**a < x ≤ b**
[a, b)	half open	**a ≤ x < b**

Reinhard Schultz
Department of Mathematics
University of California, Riverside
December, 2012

Comments on Internet resources

Traditional printed publications in mathematics are normally filtered through an editorial reviewing process which checks their accuracy (not perfectly, but for the most part very reliably). Some widely used Internet sources maintain similar standards (for example, most of the sites supported by recognized academic institutions), but others have far more lenient standards, and this fact must be acknowledged. Probably the most important single example is the ***Wikipedia*** site:

http://en.wikipedia.org/wiki/Main_Page

The ***Wikipedia*** site contains an incredibly large number of articles, with extensive information on a correspondingly vast array of subjects. The articles are written by volunteers, and in most cases they can be edited by anyone with access to the Internet, including some individuals whose views or understanding of a subject may be highly controversial or simply unreliable. This issue has been noted explicitly by ***Wikipedia*** in its articles on itself, and in particular the following discuss the matter in some detail.

http://en.wikipedia.org/wiki/Wikipedia

http://en.wikipedia.org/wiki/Reliability_of_Wikipedia

Since a few documents in this directory make references to ***Wikipedia*** articles, the underlying policies and reasons for doing so deserve to be discussed. First of all, despite the justifiable controversy surrounding the reliability of some online ***Wikipedia*** articles, the entries for standard, well – established topics in the sciences are generally very reliable, and the ones cited in the course notes were specifically checked for accuracy before they were cited. As such, they are inserted into these notes as convenient but reliable online alternatives to more traditional library references *strictly on a case by case basis*. Consequently, this usage should not be interpreted as a blanket policy of acceptance for all such articles, even in the "hard" sciences. In general, it is best to think of ***Wikipedia*** articles as merely first steps in gathering information about a subject and not as substitutes or replacements for more authoritative (printed or electronic) references in term papers or scholarly articles. All statements in ***Wikipedia*** articles definitely should be checked independently using more authoritative sources.

In any discussion of Internet references, some comments about World Wide Web searches using ***Google*** (or other search engines) are also appropriate. The extreme popularity and wide use of ***Google*** searches clearly show their value for all sorts of purposes. Of course, it is important to remember that search engines are designed to make money and that profit motives might affect the results of searches, but usually this is not a problem for topics in the sciences. Most of the time search engines are very reliable at listing the best references first, but this is not always the case, and therefore it is strongly recommended that a user should normally go beyond the first page of **10** search results. As a rule, it is preferable to look at the top **20, 50** or even **100** results.

I : General considerations

This is an upper level undergraduate course in set theory. There are two official texts.

> P. R. Halmos, ***Naive Set Theory*** (Undergraduate Texts in Mathematics). Springer – Verlag, New York, 1974. ISBN: 0–387–90092–6.

This extremely influential textbook was first published in 1960 and popularized the name for the "working knowledge" approach to set theory that most mathematicians and others have used for decades. Its contents have not been revised, but they remain almost as timely now as they were nearly fifty years ago. The exposition is simple and direct. In some instances this may make the material difficult to grasp when it is read for the first time, but the brevity of the text should ultimately allow a reader to focus on the main points and not to get distracted by potentially confusing side issues.

> S. Lipschutz, ***Schaum's Outline of Set Theory and Related Topics*** (Second Ed.). McGraw–Hill, New York, 1998. ISBN: 0–07–038159–3.

The volumes in Schaum's Outline Series are designed to be extremely detailed accounts that are written at a level accessible to a broad range of readers, and this one is no exception. As such, it stands in stark contrast to Halmos, and in this course it will serve as a workbook to complement Halmos.

The following book has also been used for this course in the past and might provide some useful additional background. It is written at a higher level than Halmos, but it is also contains very substantially more detailed information.

> D. Goldrei, ***Classic Set Theory: A guided independent study.*** Chapman and Hall, London, 1996. ISBN: 0–412–60610–0.

Still further references (***e.g.***, the text for Mathematics 11 by K. Rosen) will be given later.

These ***course notes*** are designed as a further source of official information, generally at a level somewhere between the two required texts. Comments on both Halmos and Lipschutz will be inserted into these notes as they seem necessary.

I.1 : Overview of the course

(Halmos, *Preface***; Lipschutz,** *Preface***)**

Set theory has become the standard framework for expressing most mathematical statements and facts in a formal manner. Some aspects of set theory now appear at nearly every level of mathematical instruction, and words like *union* and *intersection* have become almost as standard in mathematics as *addition*, *multiplication*, *negative* and *zero*. The purpose of this course is to cover those portions of set theory that are used and needed at the advanced undergraduate level.

In the preface to ***Naive Set Theory***, P. R. Halmos (1916 – 2006) proposes the following characterization of the set – theoretic material that is needed for specialized undergraduate courses in mathematics:

> *Every mathematician agrees that every mathematician must know some set theory; the disagreement begins in trying to decide how much is some. The purpose ... is to tell the beginning student the basic set – theoretic facts ... with the minimum of philosophical discourse and logical formalism. The point of view throughout is that ... the concepts and methods ... are merely some of the standard mathematical tools.*

Following Halmos, whose choice of a book title was strongly influenced by earlier writings of H. Weyl (1885 – 1955), mathematicians generally distinguish between the "naïve" approach to set theory which provides enough background to do a great deal of mathematics and the axiomatic approach which is carefully formulated in order to address tough questions about the logical soundness of the subject. We shall discuss some key points in the axiomatic approach to set theory, but generally the emphasis will be on the naïve approach. The following quotation from Halmos provides some basic guidelines:

> *axiomatic set theory from the naïve point of view ... axiomatic in that some axioms for set theory are stated and used as the basis for all subsequent proofs ... naïve in that the language and notation are those of ordinary informal (but formalizable) mathematics. A more important way in which the naïve point of view predominates is that set theory is regarded as a body of facts, of which the axioms are a brief and convenient summary.*

The Halmos approach to teaching set theory has been influential and has proven itself in a half century of use, but there is one point in the preface to ***Naive Set Theory*** that requires comment:

> *In the orthodox axiomatic view [of set theory] the logical relations among various axioms are the central objects of study.*

An entirely different perspective on axiomatic set theory is presented in the following online site:

http://plato.stanford.edu/entries/set-theory

Much of the research in axiomatic set theory that is described in the online site involves **(1)** the uses of set theory in other areas of mathematics, and **(2)** testing the limits to which our current understanding of mathematics can be safely pushed.

There is some overlap between the contents of this course and the lower level course *Mathematics 11: Discrete Mathematics*. Both courses cover basic concepts and terms from set theory, but there is more emphasis in the former on counting problems and more emphasis here on abstract constructions and properties of the real number system. A related difference is that there is more emphasis on finite sets in Mathematics 11. At various points in the course it might be worthwhile to compare the treatment of topics in this course and its references with the presentation in the corresponding text for Mathematics 11:

K. H. Rosen, ***Discrete Mathematics and Its Applications*** (Fifth Ed.). McGraw – Hill, New York, 2003. ISBN: 0–072–93033– 0. *Companion Web site:* http://www.mhhe.com/math/advmath/rosen/

Some supplementary exercises from this course will be taken from Rosen, and supplementary references to it will also be given in these notes as appropriate.

One basic goal of an introduction to the foundations of mathematics is to explain how mathematical ideas are expressed in writing. Therefore a secondary aim of these notes (and the course) is to provide an overview of modern mathematical notation. In particular, we shall attempt to include some major variants of standard notation that are currently in use.

At some points of these notes there will be discussions involving other areas of the mathematical sciences, mainly from lower level undergraduate courses like calculus (for functions of one or several variables), discrete mathematics, elementary differential equations, and elementary linear algebra. The reason for such inclusions is that we are developing a foundation for the mathematical sciences, and in order to see how well such a theory works it is sometimes necessary to see how it relates to some issues from other branches of the subject(s).

The most important justification for the course material is that provides a solid, relatively accessible logical foundation for the mathematical sciences and an overview of how one reads and writes mathematics. However, this does not explain how or why set theory was developed, and some knowledge of these points is often useful for understanding the mathematical role of set theory and the need for some discussions that might initially seem needlessly complicated. At various points in these notes — and particularly for the rest of this unit — we shall include material to provide historical perspective and other motivation.

Starred proofs and appendices

We shall follow the relatively standard notational convention and mark proofs that are more difficult, or less central to the course, by one to four stars. Generally the number of stars reflects a subjective assessment of relative difficulty or importance; items not marked with any starts have the highest priority, items with one star have the next highest priority, and so on. Section **V.3** is an exception to this principle for the reasons given at the beginning of that portion of the notes.

There are also several appendices to sections in the notes; these fill in mathematical details or cover material that is not actually part of the course but is closely related and still worth knowing. Since this material can be skipped without a loss of logical continuity, we have also passed on inserting stars in the appendices.

Exercises

As in virtually every mathematics course, working problems or exercises is important, and for each unit there are lists of questions, problems or exercises to study or attempt. Normally the exercises for a section will begin with a list of examples from Lipschutz called ***"Problems for study."*** Solutions for all these are given in Lipschutz, but

attempting at least some of them before looking at the solutions is strongly recommended. Each section will also have a list of "***Questions to answer***" or "***Exercises to work.***" Answers and solutions for these will be given separately.

I.2 : Historical background and motivation

It is important to recognize that mathematicians did not develop set theory simply for pedagogical or aesthetic reasons, but on the contrary they did so in order to understand specific problems in some fundamentally important areas of the subject. Three of the most important influences in the development of set theory were the following:

1. There was an increasing awareness among later 19th century mathematicians that a more secure logical framework for mathematics was needed.
2. Several 19th century mathematicians and logicians discovered the algebraic nature of some basic rules for deductive logic.
3. Most immediately, there was a great deal of research at the time to understand the representations of functions by means of trigonometric series.

The first of these reflects the *unavoidable need* for something like set theory in modern mathematics, while the second reflects the *formal structure* of set theory and the third reflects its *principal substance*, which is *the study of sets that are infinitely large*. In brief, these are the "*why*," the "*how*," and the "*what*" of set theory. We shall discuss each of these in the order listed.

At various points in this section and elsewhere in these notes, we shall refer to the text for the course ***Mathematics 153: History of Mathematics***:

> D. M. Burton, ***The History of Mathematics, An Introduction*** (Sixth Ed.). McGraw – Hill, New York, 2006. ISBN: 0– 073– 05189– 6.

The excellent online ***MacTutor History of Mathematics Archive*** located at the site

http://www-groups.dcs.st-and.ac.uk/~history/index.html

contains extensive biographical information for more than 1100 mathematicians (including many women and individuals from non-Western cultures) as well as an enormous amount of other material related to the history of mathematics.

We now begin our summary of historical influences leading to the development of set theory.

The need for more reliable logical foundations. Most areas of human knowledge are now organized using deductive logic in some fashion, and the ancient Greek formulation of mathematics in such terms was one of the earliest and most systematic examples. With the discovery of irrational numbers, Greek mathematics used geometrical ideas as their logical foundation for mathematics, and with the passage of time Euclid's ***Elements*** emerged as the standard reference. This standard for logical soundness remained

unchanged for nearly **2000** years, and the following quotation from the works of Isaac Barrow (1630 – 1677) reflects this viewpoint:

> Geometry is the basic mathematical science, for it includes arithmetic, and mathematical numbers are simply the signs of geometrical magnitude.

Barrow's viewpoint was adopted in the celebrated work, *Philosophiæ Naturalis Principia Mathematica*, written by his student Isaac Newton (1642 – 1727). On the other hand, the development of calculus in the 17th century required several constructions that did not fit easily into the classical Greek setting. In this context, it is slightly ironic that Barrow deserves priority for several important discoveries leading to calculus.

A simple — probably much too simple — description of calculus is that it is a set of techniques for working with quantities that are limits of successive approximations. Probably the simplest illustration of this is the area of a circle, which is the limit of the areas of regular n – sided polygons that are inscribed within, or circumscribed about, the circle as n becomes increasingly large. During the Fifth Century B. C. E., Greek mathematicians and philosophers discovered that a casual approach to infinite processes could quickly lead to nontrivial logical difficulties; the best known of these are contained in several well known paradoxes due to Zeno of Elea (*c.* 490 – 425 B. C. E.; see pages 103 – 104 of Burton for more details). The writings of Aristotle (384 – 322 B. C. E.) in the next century helped set a course for Greek mathematics that avoided the "horror of the infinite." When Archimedes (287 – 212 B. C. E.) solved numerous problems from integral calculus, his logically rigorous proofs of the solutions used elaborate arguments by contradiction in which he studiously avoided questions about limits.

This stiff resistance to thinking about the infinite eventually weakened, in part due to influences from Indian mathematics, which was far more open to discussing infinity, and also in part due various investigations in mathematics and philosophy during the late Middle Ages. When interest in problems from calculus reappeared towards the end of the 16th century, there were many workers in the area who used infinite processes freely, while there were also some who had reservations about some or all such techniques. Since the methods of calculus were giving reliable and consistent answers to questions that had been previously out of reach, the resolution of such misgivings was an important issue. In the discussions of this problem which took place during the 17th and 18th centuries, it had become clear that calculus involves limit concepts that are beyond normal geometrical experience. We shall not attempt to retrace the entire development of this, but instead we shall concentrate on some important developments from the 19th century. The first of these was the relatively precise definition of limit due to A. – L. Cauchy (1789 – 1857) in 1821; this was further refined into the modern definition of limit using δ and ε which is due to K. Weierstrass (1815 – 1897). Another important development was the critical analysis of convergence questions for infinite series, particularly in the writings of N. H. Abel (1802 – 1831). A third development was the realization that certain basic facts about continuous functions required rigorous logical proofs. Examples include the Intermediate Value Theorem and its proof by B. Bolzano (1781 – 1848). This listing of developments is definitely (and deliberately!) not exhaustive, but it does illustrate the 19th century activity to put the content of calculus on a logically sound foundation.

Ultimately such basic facts from calculus depend upon a firm understanding of the real numbers themselves. Greek mathematicians turned to geometry as a foundation for mathematics precisely because their understanding of the real numbers was incomplete. However, the work of Eudoxus of Cnidus (*c.* 408 – 355 B. C. E.) yielded one very important property of real numbers; namely, between any two real numbers there is a rational number. By the end of the 16th century our usual understanding of real numbers in terms of infinite decimals was a well established principle in European mathematics, science and engineering. The final insight in the process was due to R. Dedekind (1831 – 1916), and it was a converse to the principle implicitly due to Eudoxus; specifically, the real numbers are in some sense the ***largest possible number system*** in which everything can be approximated by rational number to any desired degree of accuracy. ***Justifying this viewpoint in a logically rigorous manner requires the methods and results of set theory.***

At the same time that mathematicians were developing a new logical foundation for calculus during the 18th and 19th centuries, still other advances in mathematics led to even more serious questions about the foundations of mathematics as they had been previously understood. One philosophical basis for using geometry as a foundation for mathematics is to view the postulates of Euclidean geometry as absolutely inevitable necessities of thought, much like the fact that two plus two equals four. In particular, the 18th century philosophical writings of I. Kant (1724 – 1804) were particularly influential in viewing the basic facts of geometry as intuitions that are independent of experience. When 19th century mathematicians such as J. Bolyai (1802 – 1860), N. Lobachevsky (1793 – 1856) and C. F. Gauss (1777 – 1855) realized that there was a logically consistent alternative to the axioms for Euclidean geometry, the Kantian position became far more difficult to defend. Further information on the Non – Euclidean geometry studied by these mathematicians appears on pages 561 – 601 of Burton.

The development of a mathematically rigorous treatment of calculus had an implication for classical Euclidean geometry that was largely unanticipated. When mathematicians examined classical geometry in light of the logical standards that they needed for calculus, they realized that the classical framework did not meet the new standards. For example, concepts like betweenness of points on a line and points lying on the same or different sides of a line were generally ignored in Euclid's ***Elements***. One way to illustrate the need for treating such matters carefully is to see what can go wrong if they are dismissed too casually. A standard example in this direction is the "proof" in the online reference below, which is attributed to W. Rouse Ball (1850 – 1925). This looks very much like a classical Greek proof, but it reaches the obviously false conclusion that every triangle is isosceles:

http://www.mathpages.com/home/kmath392.htm

The need to repair the foundations of classical Greek geometry further underscored the urgent need to have an entirely new logical foundation for mathematics.

In fact, the adoption of set theory as a foundation for mathematics is also a key step towards bringing classical Greek geometry up to modern logical standards. A discussion of this work is beyond to scope of these notes, but some further information is contained on pages 619 – 621 of Burton.

The use of algebraic methods to analyze logical questions. Traditionally, logic was studied as a branch of philosophy, and the ancient Greek approach to mathematics established the role and usefulness of logic in studying mathematics. Eventually mathematicians and logicians realized that, conversely, some ideas from mathematics were also useful in the analysis of logic. Some early examples of logical symbolism appear in the work of J. L. Vives (1492 – 1540) and J. H. Alsted (1588 – 1638). Fairly extended discussions appear in papers of G. W. von Leibniz (1646 – 1716) that were not published during his lifetime, and during the 18th century there were several further tentative probes in this direction by others such as Ch. von Wolff (1679 – 1754), G. Ploucquet (1716 – 1790), J. H. Lambert (1728 – 1777), and L. Euler (1707 – 1783). However, sustained and productive interest in the mathematical aspects of logic began in the middle of the 19th century, and since that time mathematical ideas have played a very important (but not exclusive) role in this subject. More recently, the importance of formal logic for computer science has been a major source of motivation for further research.

The name *mathematical logic* is due to G. Peano (1858 – 1932), and the subject is also often called symbolic logic (although not everyone necessarily agrees these terms have identical meanings). Mathematical logic still includes the logic of classical civilizations, for example as summarized in the ***Organon*** of Aristotle or the ***Nyaya Sutras*** of the Indian Philosopher Aksapada Gautama (conjecturally around the Second Century B. C. E., but possibly as early as 550 B. C. E. or as late as 150 A. D.), or the logic that was developed in ancient Chinese civilization probably around the time of Aristotle, but it is developed more like a branch of abstract algebra.

The emergence of mathematical methods as an important factor in logic was firmly established with the appearance of the book, ***The Mathematical Analysis of Logic***, by G. Boole (1815 – 1864) in 1847. Boole's work contained a great deal of new material, but in some respects it also drew upon earlier discoveries, writings and ideas due to R. Whately (1787 – 1863), G. Peacock (1791 – 1858), G. Bentham (1800 – 1884, better known for his work as a botanist), A. De Morgan (1806 – 1871) and William Stirling Hamilton (1788 – 1856); it should be noted that the latter was a Scottish logician and not the same person as the better known Irish mathematician William Rowan Hamilton (1805 – 1865), who is recognized for several fundamental contributions to mathematics, including his mathematical approach to classical physics and the invention of quaternions. The following is a typical example of a conclusion that followed from the methods of these 19th century logicians but not from classical Aristotelian logic:

> In a particular group of people,
>
> **(1)** most people have shirts,
> **(2)** most people have shoes;
>
> **therefore,** some people have both shirts and shoes.

Other contributors during the second half of the 19th century included J. Venn (1834 – 1923), who devised the pictorial representations of sets that now carry his name, and C. L. Dodgson (1832 – 1898), who is better known by his literary pseudonym *Lewis Carroll*. His interests covered a very broad range of topics, and his mathematical achievements include some deep studies in symbolic logic and logical reasoning. Much of this work involved specific logical problems of a somewhat whimsical nature, but he also made some noteworthy contributions in more general directions, including the use of truth

tables. All this activity in logic led to fairly definitive algebraic formulations by W. S. Jevons (1835 – 1882) and E. Schröder (1841 – 1902).

Further discussion of the work of Boole and De Morgan (as well as other topics that are mentioned above) appears on pages 643 – 647 of Burton.

Representations of functions by trigonometric series. Several distinct areas in mathematical physics — most notably, wave motion and heat flow — motivated interest in expressing periodic functions satisfying $f(x + 2\pi) = f(x)$ by means of an infinite series of trigonometric functions

$$f(x) \sim \frac{a_0}{2} + \sum_{n=1}^{\infty} (a_n \cos nx + b_n \sin nx)$$

analogous to the power series expansions of the form

$$\sum_{i=0}^{\infty} a_i z^i,$$

that are so useful for many purposes. A discussion of such series at the level of first year calculus appears in Sections 8.9 and 8.10 of the following classic calculus text:

> R. L. Finney, M. D. Weir, and F. R. Giordano. ***Thomas' Calculus, Early Transcendentals*** (Tenth Ed.). Addison – Wesley, Boston, 2000. ISBN: 0–201–44141–1.

During the middle of the 19th century many prominent mathematicians studied aspects of the following question:

> *To what extent is the representation of a function by a (possibly infinite) trigonometric series unique?*

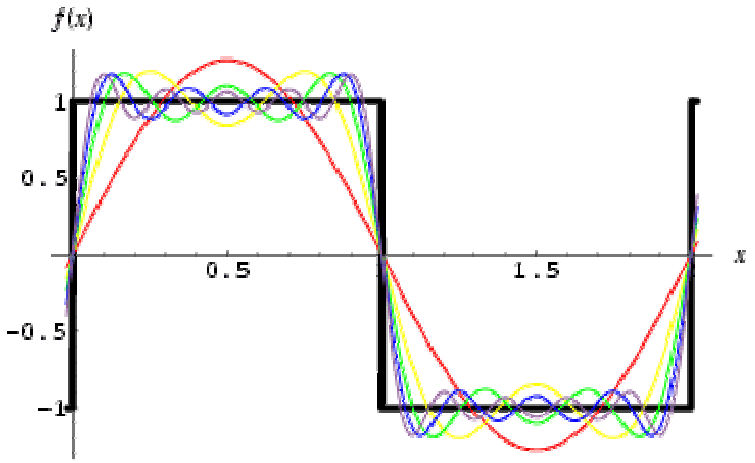
The founder of set theory, **Georg Cantor** (1845 – 1918), gave a positive answer to this question in 1870.

Theorem. *Suppose that we are given two expansions of a reasonable function f as a convergent trigonometric series:*

$$f(x) = \tfrac{1}{2}a_0 + \sum_{n=1}^{\infty} a_n \cos(nx) + \sum_{n=1}^{\infty} b_n \sin(nx) = \tfrac{1}{2}a_0' + \sum_{n=1}^{\infty} a_n' \cos(nx) + \sum_{n=1}^{\infty} b_n' \sin(nx)$$

Then $a_n = a_n'$ and $b_n = b_n'$ for all nonnegative integers n.

This is a pretty good conclusion, but one actually would like a little more. We have not specified what we mean by a reasonable function, and indeed we should like to include some functions that are not necessarily continuous. The most basic example in this context is the so – called ***square wave function*** whose value from 0 to π is $+1$ and whose value from π to 2π is -1. Waves of this type occur naturally in several physical contexts: The graph of the square wave function (with the x – axis rescaled in units of π) is given below.



(***Source:*** http://mathworld.wolfram.com/FourierSeriesSquareWave.html)

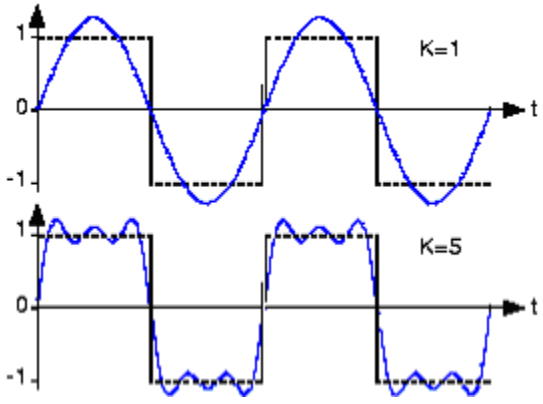
Obviously this function is discontinuous, with a jump in values at every integral multiple of π, and one might suspect that it really does not matter how we might define the function at such sparsely distributed jump discontinuities. In fact, this is the case, and for every such choice one obtains the same trigonometric series representing the square wave function:

$$f(x) = \frac{4}{\pi} \sum_{n=1,3,5,\ldots}^{\infty} \frac{1}{n} \sin\left(\frac{n\pi x}{L}\right).$$

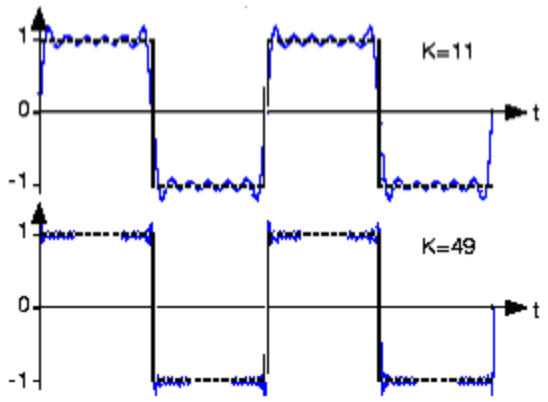
(This is the general expression for period $2L$, so here $L = \pi$.)

Here are some graphs to show how close the partial sums come to approximating the square wave. Note that the graphs suggest the value of the infinite sum is zero at integral multiples of π (this is in fact true, but we shall not go into the details). Here is a reference for these illustrations.

http://cnx.rice.edu/content/m0041/latest/



(***continued on the next page***)



Clearly we could carry out the same construction for higher frequency square waves (using positive integral multiples of 2π) and find examples of reasonable functions with the same trigonometric series such that the values of the functions are the same except for some arbitrarily large finite set of values between 0 and 2π. This leads naturally to the following problem that Cantor considered in connection with his basic uniqueness result:

> *Do two reasonable functions have the same Fourier series if they agree at all but an infinite sequence of points p_n between 0 and 2π?*

Cantor showed that the answer was ***yes*** if the sequence had the following ***closure property:*** *If a subsequence $p_{n(k)}$ converges to a limit L, then $L = p_m$ for some m.*

Subsequent work established the result without the closure hypothesis. Further information on these matters may be found in the following reference (which is definitely ***not*** written at the advanced undergraduate level — the citation is included for the sake of completeness):

> A. S. Kechris and A. Louveau, ***Descriptive set theory and the structure of sets of uniqueness*** (London Math. Soc. Lect. Notes Vol. 128). Cambridge University Press, Cambridge, UK, and New York, 1987. ISBN: 0–521–35811–6.

The important point of all this for our purposes is that Cantor's analysis of the exceptional points led him to abstract set – theoretic concepts and ultimately to his extremely original (and at first highly controversial) research on set theory. Additional information on Cantor and his work appears on pages 668 – 690 of Burton. Further developments in the history of set theory are discussed on pages 690 – 707 of Burton, but the material covered after the middle of page 701 is not discussed in this course.

Some further references

Additional historical background on the topics discussed in this section is given in the following online sites.

http://math.ucr.edu/~res/math153/history03.pdf

This site discusses some issues related to the logical gaps in Euclid's ***Elements*** and why the latter should be still be viewed very positively despite such problems**.**

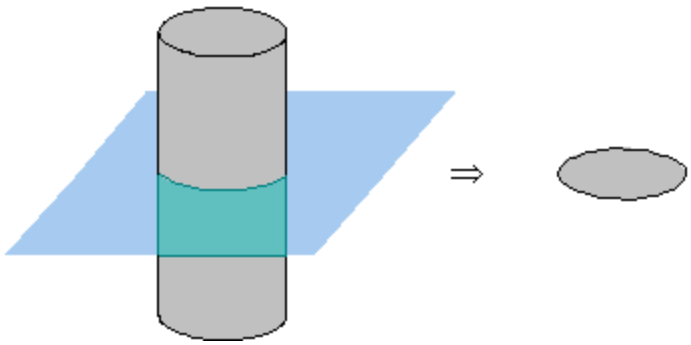
http://math.ucr.edu/~res/math153/history12.pdf

http://math.ucr.edu/~res/math153/history14a.pdf

The first document contains an account of infinitesimals which goes beyond the Appendix to this section in some respects**,** and it also includes further discussion on problems with the logical soundness of calculus that arose during the period from 1600 to 1900**.** The second document describes one noteworthy example to illustrate how an overly casual approach to manipulating infinite series can lead to fallacious conclusions**.**

I.2. Appendix : Comments on infinitesimals

One of the major logical problems with calculus as developed in the 17th century was the legitimacy of objects called ***infinitesimals***. The idea is well illustrated in the method employed by B. Cavalieri (1598 – 1647) to study the volume of a solid **A** that is contained between two parallel planes. If the planes are defined by the equations $z = 0$ and $z = 1$**,** then for each **t** between 0 and 1 one has the cross section $\mathbf{A}_t$ formed by intersecting **A** with the parallel plane defined by $z = t$**.** Cavalieri's idea is to view **A** as composed of an infinite collection of cylindrical solids whose bases are the cross sections $\mathbf{A}_t$ and whose heights are some very small**,** in fact ***infinitesimally small***, value that we shall call **dt.**



(**Figure source**: http://www.mathleague.com/help/geometry/3space.htm)

From this viewpoint, the total volume is obtained by adding the volumes of these infinitesimally short cylindrical solids; in modern terminology, one adds or integrates these infinitesimals by taking the definite integral of the area function with respect to **t** from 0 to 1**.** Of course**,** the point of this discussion is to convince the reader that the volume of **A** is given by the following standard integral formula in which **a(t)** denotes the area of the planar section $\mathbf{A}_t$**:**

$$V = \int_0^1 a(t)\,dt$$

This is an excellent heuristic argument, but its logical soundness depends upon describing the concept of an infinitesimal precisely. It was clear to 17th and 18th century scientists and philosophers that such infinitesimals were supposed to be smaller than any finite quantity but were still supposed to be positive. If one is careless with such a notion it is easy to contradict the principle that between any two real numbers there is a rational number; a crucial question is *whether it is* **ever** *possible to be careful enough to avoid these or other logical difficulties*. Although proponents of calculus made vigorous efforts to explain infinitesimals and were getting reliable answers, their explanations did not really clarify the situation much to mathematicians or others of that era. A clear and rigorous foundation for calculus was not achieved until infinitesimals were discarded (for foundational purposes) in the 19th century and the subject was based upon the concept of limit (see the discussion above).

Despite their doubtful logical status, many users of mathematics have continued to work with infinitesimals, probably motivated by their relative simplicity, the fact that they gave reliable answers, and an expectation that mathematicians could ultimately find a logical justification for whatever was being attempted. This attitude towards infinitesimals was also evident in many undergraduate textbooks in mathematics, science and engineering, particularly through the first half of the 20th century; the following is a typical example:

> W. A. Granville, P. F. Smith and W. R. Longley, ***Elements of Differential and Integral Calculus*** (Various editions from 1904 to 1962). Wiley, New York, 1962. ISBN: 0–471–00206–2.

During the nineteen sixties Abraham Robinson (1918 – 1974) used extensive machinery from set theory and abstract mathematical logic to prove that one can in fact construct a number system with infinitesimals that satisfy the expected formal rules. However, the crucial advantage of Robinson's concept of infinitesimal — its logical soundness — is balanced by the fact that, unlike 17th century infinitesimals, it is neither simple nor intuitively easy to understand. The associated theory of ***Nonstandard Analysis*** has been studied to a considerable extent mathematically, but it is not widely used in the traditional applications of the subject to the sciences and engineering; on the other hand, some recent work in mathematical economics has been formulated within the context of nonstandard analysis. The following online references provide further information on this subject:

http://members.tripod.com/PhilipApps/nonstandard.html

http://www.haverford.edu/math/wdavidon/NonStd.html

http://mathforum.org/dr.math/faq/analysis_hyperreals.html

http://en.wikipedia.org/wiki/Nonstandard_analysis

http://www.math.uiuc.edu/~henson/papers/basics.pdf

Here are a few textbook references for nonstandard analysis:

> J. M. Henle and E. M. Kleinberg, ***Infinitesimal Calculus.*** Dover Publications, New York, 2003. ISBN: 0 – 486 – 42886– 9.
>
> J. L. Bell, ***A Primer of Infinitesimal Analysis***. Cambridge University Press, New York, 1998. ISBN: 0 – 521– 62401– 0.
>
> A. E. Hurd and P. A. Loeb, ***An Introduction to Nonstandard Real Analysis*** (Pure and Applied Mathematics, Vol. 118). Academic Press, Orlando, FL, 1965. ISBN: 0 – 123 – 62440 – 1.

Comment on "differential" notation

In older mathematics texts and also some newer books in other subjects, expressions like dx, dy and df refer to infinitesimals. However, in newer mathematics books, for example the multivariable calculus text

> J. E. Marsden and A. Tromba, ***Vector Calculus*** (Fifth Ed.). Freeman, New York, 2003. ISBN: 0–716–74992–0.

such symbols generally have a much different meaning, and it is important to recognize this. A precise description of the current usage is beyond the scope of this course; one general suggestion is to check a textbook carefully if it contains expressions like dx and dy standing by themselves and not part of a larger expression for a derivative or an integral. This applies particularly to any mathematics book beyond first year calculus with a first edition date after 1950.

Logical rigor and modern mathematical physics

The development of nonstandard analysis during the second half of the 20th century is definitely not the final step to putting everything related to mathematics on a logically sound basis; in fact, one expects that advances in the other sciences — particularly in physics — are likely to continue yielding new ideas on how our mathematical concepts might be stretched to deal effectively with new classes of problems. Probably the most important subject currently requiring a mathematically rigorous description is the formalism introduced by the renowned physicist R. P. Feynman (1918 – 1988) about 60 years ago to study questions in quantum electrodynamics. The value and effectiveness of Feynman's techniques in physics — and even in some highly theoretical areas of mathematics — are very widely recognized, but currently there is no general method to provide rigorous mathematical justifications for the results predicted by Feynman's machinery (however, it is possible to do so in a wide range of special cases). A comprehensive account of the mathematical aspects of Feynman's ideas is given in the book cited below, and the accompanying online references provide quick surveys of Feynman's life and work:

> G. W. Johnson and M. L. Lapidus, ***The Feynman Integral and Feynman's Operational Calculus*** (Oxford Mathematical Monographs, Corrected Ed.). Oxford Univ. Press, Oxford, UK, and New York, 2002. ISBN: 0–19–851572–3.

http://en.wikipedia.org/wiki/Richard_Feynman

http://www.feynman.com/

http://www2.slac.stanford.edu/vvc/theory/feynman.html

I.3 : Selected problems

We shall begin with an online quotation from the site

http://en.wikipedia.org/wiki/Adjoint_functor

on introducing abstract concepts.

> *Concepts are judged according to their use in solving problems, at least as much for their use in building theories.*

Here is a more focused version of the quotation:

> ***Ideally, an abstract mathematical construction such as set theory should answer, or at least shed useful new light, on some problem(s) of recognized importance.***

Motivated by the preceding comments, we shall list a few mathematical questions of varying importance and difficulty as test cases for the usefulness of set theory.

1. Providing a clear and simple mathematical description of both relations and functions.
2. Rigorously justifying the so – called ***pigeonhole principle*****:** If we are given **m** objects and **n** locations to put them with **m > n,** then at least one of the locations will contain at least two objects.
3. Finding a mathematically efficient and logically sound description of the real number system.
4. Understanding the likelihood that a real number which is "chosen at random" will be ***algebraic;*** *i.e.*, it is the root of a nonconstant polynomial equation with integral coefficients.

Given the fundamental importance of the real number system to analysis, it should be apparent that ***anything which will make the latter logically rigorous will play a key role in the foundations of mathematics.***

At this point a few additional remarks about the desired formulation of the real number system seem appropriate. Even though we view real numbers in terms of their infinite decimal expansions, we do not want our mathematical description of real numbers to be phrased in such terms. There are two reasons for this. One is that verifying algebraic identities for infinite decimal expansions is at best awkward; for example, consider the practical and theoretical difficulties in writing out the reciprocal to an infinite decimal expansion between $\mathbf{0}$ and $\mathbf{1}$ or writing out the positive square root of such a number. A second reason is that we would like our concept of real number to be independent of any choice of computational base, and in particular we would like a system that does not change if we replace base $\mathbf{10}$ by, say, base $\mathbf{2}$ (or $\mathbf{8,}$ or $\mathbf{12,}$ or $\mathbf{16,}$ or $\mathbf{60,}$ or **…**).

In an appendix to the final section of these notes we shall also consider one further question that arises naturally in connection with the points covered in this unit; namely, formulating repaired versions of classical Greek deductive geometry in terms of modern set theory.

II : Basic concepts

This unit is the beginning of the strictly mathematical development of set theory in the course. We begin with a brief discussion of how mathematics is written and continue with a summary of the main points in logic that arise in mathematics. The latter is mainly meant as background and review, and also as a reference for a few symbols that are frequently used as abbreviations. In the remaining sections we introduce the most essential notions of set theory and some of their simplest logical interrelationships.

Mathematical language

> Mathematicians are like Frenchmen; whatever you say to them they translate into their own language and forthwith it is something entirely different.
>
> J. W. von Goethe (1749 – 1832)

A page of mathematical writing is different from a page of everyday writing in many respects, and for an inexperienced or uninitiated reader it is often more difficult to understand. Before considering strictly mathematical topics in these notes, it might be helpful to summarize some special features of mathematical language and the reasons for such differences.

The language of mathematics is a special case of ***technical language*** or ***language for special purposes.*** As such, it has many things in common with other specialized language uses in the other sciences and also in legal writing.

In all these contexts, it is important to state things precisely and to justify assertions based upon earlier writing. It is also important to avoid things which are unrelated to the substance of the discussion, including emotional appeals and nearly all personal remarks; when the latter appear, they are usually restricted to a small part of the text.

The need for precise, impersonal language affects mathematical writing in several ways. We shall list some notable features below.

1. Sentences tend to be long and carefully written, sometimes at the expense of clarity. This is often necessary to avoid misunderstandings or to eliminate potential sources for errors. For example, in mathematics when one divides a number **x** by a number **y**, it is necessary to stipulate that **y** be nonzero.
2. In scientific writing there is more of a tendency to stress nouns and modifiers rather than verbs, and there is a much greater use of the passive voice. For example, instead of saying, "You can do **X**," one generally sees the more impersonal, "It is possible to do **X**." This reinforces the unimportance or anonymity of the individual who does **X**. However, a reader who is not used to such an impersonal style might view it as uninviting.

3. Precise meanings must be attached to specific words. These do not necessarily correspond to a word's everyday meaning(s), and of course there are also many words that are rarely if ever seen elsewhere. Words like "product" and "set" and "differentiate" are examples of words whose mathematical meanings differ from standard usage. Other words such as "abelian" or "eigenvector" or "integrand" are essentially unique to mathematics and only appear when mathematics is presented or applied to another subject.
4. There is an extensive use of references to the writings of others. Such citations are logically indispensable and make everything more concise, but they can also make it difficult or impossible to read through something without frequent interruptions.
5. Particularly in the sciences, there is a heavy reliance on symbols such as numerals, operators (for example, the plus and equals signs), formulas or equations, and diagrams as well as other graphics. These allow the writer to express many things quickly but precisely. However, they may be difficult to decipher, particularly for a beginner.

The pros and cons of mathematical (and other scientific) language are reflected by a surprising fact: Even though such material is more difficult to read than an ordinary book, it is much easier to translate scientific writings to or from a foreign language than it is to translate a best selling novel or a regular column in a newspaper. In particular, adequate computerized translations of scientific articles are considerably easier to produce than acceptable computerized translations of literature (try using software like http://babelfish.yahoo.com/ to translate some passages and see what happens).

Both clarity and preciseness are important in mathematical (and other scientific) writing. A lack of precision can lead to costly mistakes in scientific experiments and engineering projects (similar considerations apply to legal writing, where ambiguities involving simple words can lead to extensive and expensive litigation). On the other hand, a lack of clarity can undermine the fundamental goals of communicating information. Every subject has tried to adopt guidelines for balancing these contrasting aims, but probably there will always be challenges to doing so effectively in all cases.

II.1 : Topics from logic

(Lipschutz, §§ 10.1 – 10.12)

Mathematics is based upon logical principles, and therefore some understanding of logic is required to read and write mathematics correctly. In this course we shall take the most basic concepts of logic for granted. Our main purpose here is to describe the key logical points and symbolic logical notation that will be used more or less explicitly in this course. Chapter 10 of Lipschutz contains numerous examples illustrating the main points of logic that we shall use in this course, and it it provides additional background and reference material. Sections 1.1 – 1.5 of Rosen also treat these topics in an introductory but systematic manner.

In most mathematical writings, the logical arguments are carried out using ordinary language and standard algebraic symbolism. When logical terminology as developed in

this section is used, it is often used intermittently for purposes of abbreviation when ordinary wording becomes too lengthy or awkward; there are similarities between this and the practice of explaining some programming issues in a pseudo – code that is halfway between ordinary and computer language. Although such logical abbreviations are only used sometimes in mathematics, it is important to be familiar with them and recognize them when they do appear.

Concepts from propositional calculus

The basic objects in propositional calculus are simple declarative sentences, and by convention each sentence is either true or false. There are several simple grammatical and logical operations that can be used to connect sentences.

1. If **P** and **Q** are sentences, then the sentence **P *and* Q** is sometimes called the **conjunction** of **P** and **Q**, and it is symbolically denoted by either $\mathbf{P} \wedge \mathbf{Q}$ or the less formal **P & Q.** Of course, if **P** and **Q** are both true, then $\mathbf{P} \wedge \mathbf{Q}$ is true, while if one or both of **P** and **Q** are false, then $\mathbf{P} \wedge \mathbf{Q}$ is false.
2. If **P** and **Q** are sentences, then the sentence **P *or* Q** is sometimes called the **disjunction** of **P** and **Q**, and it is denoted symbolically by $\mathbf{P} \vee \mathbf{Q}$. In mathematics we use an ***inclusive* OR *connective***; ***i.e.***, the statement $\mathbf{P} \vee \mathbf{Q}$ is true when **P** is true or **Q** is true, or both are true, and $\mathbf{P} \vee \mathbf{Q}$ is false only when both **P** and **Q** are false.
3. If **P** is a sentence, then the sentence ***not* P** is sometimes called the **negation** of **P**, and it is denoted symbolically by $\neg$ **P** or **– P** or ***~P*** (still other symbolisms are also used). As one would expect, the sentence $\neg$ **P** is false when **P** is true, and the sentence $\neg$ **P** is true when **P** is false.
4. If ***P*** and ***Q*** are sentences, the **conditional** sentence ***if* P*, then* Q** is denoted symbolically by $\mathbf{P} \rightarrow \mathbf{Q}$ or $\mathbf{P} \Rightarrow \mathbf{Q}$. In this conditional sentence **P** is called the **antecedent** and **Q** is called the **consequent.** Such a conditional sentence is true unless **P** is true and **Q** is false, and it is false in this case. (The truth of the conditional statement if **P** is false may seem puzzling, but one way to think about it is that since **P** is false the conditional is basically an empty statement).

Of course, one can use the preceding connectives to define new ones in other ways, and one example is the ***exclusive* OR *connective***: If **P** and **Q** are sentences, then the sentence **P *xor* Q** should have the property that **P *xor* Q** is false when **P** and **Q** are either both true or both false, and **P *xor* Q** is true otherwise. Symbolically one can write this connective in terms of the others by the formula $(\mathbf{P} \vee \mathbf{Q}) \wedge \neg (\mathbf{P} \wedge \mathbf{Q})$.

Another important operation is the standard ***if and only if connective.*** If ***P*** and ***Q*** are sentences, the **biconditional** sentence **P *if and only if* Q*,*** which is sometimes also written **P *iff* Q*,*** is given by $(\mathbf{P} \Rightarrow \mathbf{Q})$ **&** $(\mathbf{Q} \Rightarrow \mathbf{P})$, and its symbolically abbreviation is $\mathbf{P} \Leftrightarrow \mathbf{Q}$. As expected, this statement is true if both **P** and **Q** are true or both are false, and it is false if exactly one of **P** and **Q** is true and exactly one is false. The phrase **P *is***

logically equivalent to **Q** is also used frequently in mathematical writings to denote the biconditional $P \Leftrightarrow Q$.

Tautologies

By definition, a ***tautology*** is a sentence that is true no matter what the truth values are for the constituent parts. One simple example of this is $P \Rightarrow P \vee Q$. Here are several others:

1. $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$ *Law of the contrapositive*
2. $[P \wedge (P \Rightarrow Q)] \Rightarrow Q$ *Law of modus ponens*
3. $[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$ *Law of Syllogism*
4. $\neg (P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$
5. $\neg (P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q)$ *DeMorgan's Laws*
6. $\neg (P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q)$
7. $(P \Rightarrow Q) \Leftrightarrow (\neg P \vee Q)$
8. $(P \wedge Q) \Rightarrow P$
9. $\neg (\neg P) \Leftrightarrow P$
10. $(P \wedge Q) \Rightarrow (P \vee Q)$
11. $(P \Rightarrow \neg Q) \Rightarrow (Q \Rightarrow \neg P)$
12. $[\neg P \Rightarrow (R \wedge \neg R)] \Rightarrow P$ *Law of proof by contradiction*
13. $[(P \wedge \neg Q) \wedge (R \wedge \neg R)] \Rightarrow (P \Rightarrow Q)$ *Law of proof by contradiction*
14. $P \wedge \neg P$ *Law of the Excluded Middle*
15. $P \Rightarrow P$
16. $P \Leftrightarrow P$
17. $[P \Rightarrow (Q \wedge R)] \Rightarrow [(P \wedge \sim Q) \Rightarrow R]$
18. $[(P \Rightarrow S_1) \wedge (S_1 \Rightarrow S_2) \wedge \ldots \wedge (S_{n-1} \Rightarrow S_n) \wedge (S_n \Rightarrow R)] \Rightarrow (P \Rightarrow R)$ *Extended Law of Syllogism*
19. $[(P \Rightarrow R) \wedge (Q \Rightarrow R)] \Rightarrow [(P \vee Q) \Rightarrow R]$ *Proof by Cases*
20. $(P \wedge Q) \Leftrightarrow (Q \wedge P)$
21. $(P \vee Q) \Leftrightarrow (Q \vee P)$ *Commutative Laws*
22. $[P \Rightarrow (R \Rightarrow Q)] \Leftrightarrow [(P \wedge R) \Rightarrow Q]$
23. $[P \wedge (Q \wedge R)] \Leftrightarrow [(P \wedge Q) \wedge R]$
24. $[P \vee (Q \vee R)] \Leftrightarrow [(P \vee Q) \vee R]$ *Associative Laws*
25. $[P \wedge (Q \vee R)] \Leftrightarrow [(P \wedge Q) \vee (P \wedge R)]$
26. $[P \vee (Q \vee R)] \Leftrightarrow [(P \vee Q) \wedge (P \vee R)]$ *Distributive Laws*
27. $[(P \Leftrightarrow Q_1) \wedge \ldots \wedge (Q_{n-1} \Leftrightarrow Q_n) \wedge (Q_n \Leftrightarrow Q)] \Rightarrow (P \Leftrightarrow Q)$

Propositional calculus is covered in Sections 10.1 – 10.10 of Lipschutz and Sections 1.1 and 1.2 of Rosen. The material in these sections on the order of logical operations, translating English sentences and logic puzzles goes beyond the topics covered here.

Predicate calculus and quantifiers

Propositional calculus views sentences as units, and predicate calculus views ordinary declarative sentences as consisting of two main grammatical parts — the ***subject*** and

the ***predicate.*** The subjects (or ***variables***) of such sentences are generally denoted by small letters like an x, and the predicates are denoted by functions like **P(...),** the idea being that given a predicate shell one can insert an arbitrary subject to obtain a grammatically admissible sentence $\mathbf{P}(x)$ which is either true or false. A typical example of such a sentence $\mathbf{P}(x)$ might be $x + 2 = 5$. For this example we know that $\mathbf{P}(3)$ is true but $\mathbf{P}(4)$ is false. Of course, ordinary sentences may have compound subjects, and it is essential to allow logical predicates to have this property also. As one might expect, we shall denote the sentence obtained from insertion of $x_1, \ldots, x_n$ into the predicate **P** by $\mathbf{P}(x_1, \ldots, x_n)$.

We now turn to a discussion of **<u>quantifiers</u>**. Sentences involving phrases like ***For every ...*** and ***There exists ...*** play a very important role in mathematically reasoning.

The logical symbol ∀, which is called the **universal quantifier,** is a symbolic shorthand for phrases such as *<u>For each</u>*, *<u>For every</u>*, and *<u>For all</u>*. A predicate sentence such as

For every x, $\mathbf{P}(x)$

is then written symbolically as either $\forall x \;\; \mathbf{P}(x)$ or equivalently $\forall x, \mathbf{P}(x)$. Here is a typical example of a true sentence in this form:

$\forall x$, if x is a real number then x^2 is nonnegative.

The logical symbol ∃, which is called the **existential quantifier,** is a symbolic shorthand for phrases such as *<u>There exists</u>*, *<u>There is at least one</u>*, *<u>For at least one</u>*, and *<u>For some</u>*. A sentence such as ***There exists an*** x ***such that*** $\mathbf{P}(x)$ is then written symbolically as either $\exists x \;\; \mathbf{P}(x)$ or equivalently $\exists x, \mathbf{P}(x)$. Here is a typical example of a true sentence in this form:

$\exists x$, if x is a real number then $1 - x^2$ is nonnegative.

Note that if **P** is the predicate in the sentence above, then $\exists x, \mathbf{P}(x)$ is true (take $x = ½$) but $\forall x, \mathbf{P}(x)$ is false (take $x = 2$). On the other hand, for every predicate **Q** we know that $\forall x \;\; \mathbf{Q}(x)$ automatically implies $\exists x \;\; \mathbf{P}(x)$.

Since we are discussing tautologies involving quantifiers, we should mention two other basic statements of this type.

Tautology Criterion 1: *Every sentence of the type* $[\neg\exists x, \mathbf{P}(x)] \Leftrightarrow [\forall x, \neg\mathbf{P}(x)]$ *is true.*

Tautology Criterion 2: *Every sentence of the type* $[\neg\forall x, \mathbf{P}(x)] \Leftrightarrow [\exists x, \neg\mathbf{P}(x)]$ *is true.*

In mathematical writings one often sees a variant of the existential quantifier called the ***unique existential quantifier***, which is denoted by $\exists \mathbf{!}$ or $\exists !$ or $\exists \mathbf{1}$ and signifies the ***unique existence*** of some object. For example, the sentence $\exists \mathbf{!}\, x, \mathbf{P}(x)$ is true when $\mathbf{P}(x)$ is given as follows:

x is an integer and $x + 1 = 2$.

On the other hand, the sentence $\exists \mathbf{!}\, x, \mathbf{Q}(x)$ is false if $\mathbf{Q}(x)$ is given as follows:

$$x \text{ is an integer and } x^2 - 3x + 2 = 0.$$

Formally one can express $\exists!$ directly in terms of the other quantifiers because a statement of the form $\exists! x, P(x)$ can be written in the following equivalent terms:

$$[\exists x, P(x)] \;\; \& \;\; [\forall x \, \forall y, \; \{P(x) \; \& \; P(y)\} \Rightarrow \{x = y\}]$$

Another point about quantifiers that merits discussion is the order in which they are listed. If an expression contains multiple quantifiers, the order in which they appear may be very important. For example, suppose that $P(x, y)$ is the following statement:

$$x \text{ is a real number, and if } y \text{ is a real number then } x > y.$$

Then $\forall y \, \exists x, \; P(x, y)$ means that for every real number x there is a larger real number y, and hence the quantified statement is ***true***, but $\exists x \, \forall y, \; P(x, y)$ is ***false*** (there is no number x which is greater than every number, including itself). In contrast, if **P** is a predicate such that $\exists x \, \forall y, \; P(x, y)$ is true, then $\forall y \, \exists x, \; P(x, y)$ will ***always*** be true.

Predicate calculus is covered in Section 10.11 of Lipschutz and Sections 1.3 and 1.4 of Rosen. The material in these sections on bound variables, nested quantifiers, the order of quantifiers, translating English sentences and Lewis Carroll's logical puzzles goes beyond the topics covered here and in this course.

Formal structure of languages

The predicate calculus is an important first step in studying the formal structure or syntax of the language needed to carry out logical processes. The study of such structure is particularly important in some aspects of computer science. A detailed discussion of this topic is beyond the scope of these notes, but a good introductory discussion appears in Section 11.1 of Rosen. It is extremely interesting to note that much of the work on formal grammars by noted workers in computer science such as J. Backus (1924 – 2007) — who developed of the **FORTRAN** programming language which revolutionized computer programming — was anticipated many centuries earlier in the profound analysis of Sanskrit grammar due to Panini (520 – 460 B. C. E.) in his ***Astadhyayi*** (or ***Astaka***). It is particularly noteworthy that Panini's notation is equivalent in its power to that of Backus, and it has many similar properties.

Mathematical proofs

Standard methods and strategies for mathematical proofs are discussed in Sections 1.5, 3.1 and 3.3 of Rosen. We shall summarize the main points from these sections, mention a few other points points not specifically covered in these citations, and give some examples from high school mathematics and calculus (we are simply trying to illustrate the techniques, so our setting for now is informal, and in particular for the time being we shall not worry about things like how one proves the Intermediate Value Theorem that plays such an important role in calculus). This is technically an example of a concept called ***local deduction***, in which one only shows how to get from point **A** to point **B**, postponing questions about reaching point **A** to another time or place.

Some proofs use ***direct arguments***, while others use ***indirect arguments.*** The direct arguments are often the simplest, and many simple problem solving methods from elementary mathematics (algebra, in particular) are really just simple examples of direct proofs.

Example. If $2x + 1 = 5$, show that $x = 2$. **SOLUTION:** If $2x + 1 = 5$, then by subtracting 1 from each side we obtain $2x = 4$. Next, if we divide both sides of the equation $2x = 4$ by 2, we obtain $x = 2$.

In contrast, and indirect argument usually involves considering the negation of either the hypothesis or the conclusion. This generally involves ***proof by contradiction***, in which one assumes the conclusion is false and then proves part of the hypothesis is false, and it is related to the law of the ***contrapositive***: A statement **P** $\Rightarrow$ **Q** is true if and only if the *contrapositive* statement **not Q** $\Rightarrow$ **not P** is true.

A general "rule of thumb" is to consider using an indirect argument if either no way of using a direct argument is apparent or if a direct approach seems to be getting very long and complicated. There is no guarantee that an indirect argument will be any better, but if you get stuck trying a direct approach there often is not much to lose by seeing what happens if you try an indirect approach; in some cases, attempts to give an indirect argument may even lead to a valid or better direct proof.

Example. Show that if **L** and **M** are two lines then they have at most one point in common. **SOLUTION:** Suppose the conclusion is false, so that **x** and **y** are two distinct points on both **L** and **M**. Then both **L** and **M** are lines containing these two points. Since there is only one line **N** containing the two distinct points **x** and **y**, we know that **L** must be equal to **N** and similarly **M** must be equal to **N**, which means that **L** and **M** must be equal. This contradicts our original assumption; the problem arose because we added an assumption that **x** and **y** belonged to both lines. Therefore **L** and **M** cannot have two (or more) points in common.

An important step in such indirect arguments is to ***make sure that the negation of the conclusion is accurately stated.*** Mistakes in stating the negation usually lead to mistakes in arguments intended to prove the original result.

Forward and backwards reasoning. Very often it is helpful to work backwards as well as forwards. For example, if you want to show that **P** implies **Q**, in some cases it might be easier to find some statement **R** that implies **Q**, and then to see if it is possible to prove that **P** implies **R**. Of course, there may be several intermediate steps of this type.

Example. Show that the polynomial $f(x) = x^5 - x - 1$ has a real root. **SOLUTION:** We know that polynomials are continuous and that continuous functions have the Intermediate Value Property. Therefore if we can show that the polynomial is positive for some value of x and negative for another, then we can also show that this polynomial has a real root. One way of doing this is simply to calculate the value of the polynomial for several different values of the independent variable. If we do so, then we see that $f(1) = -1$ and $f(2) = 29$. Therefore we know that $f(x)$ has a root, and in fact by the Intermediate Value Theorem from first year calculus we know there is a root which lies somewhere between 1 and 2.

Proofs by cases. Frequently it is convenient to break things up into all the different cases and to check them individually, and in some cases this is simply unavoidable.

Example. Let $\mathbf{sgn}(x)$ be the function whose value is 1 if x is positive, -1 if x is negative, and 0 if $x = 0$. Prove that $\mathbf{sgn}(xy) = \mathbf{sgn}(x)\,\mathbf{sgn}(y)$.

There are three possibilities for x (positive, negative, zero) and likewise for y, leading to the following list of nine possibilities for x and y:

$$[+, +],\ [+, 0],\ [+, -],\ [0, +],\ [0, 0],\ [0, -],\ [-, +],\ [-, 0],\ [-, -]$$

One can then handle each case (or various classes of cases) separately; for example, the five cases where at least one number is zero follow because in all these cases we have $xy = \mathbf{sgn}(x)\mathbf{sgn}(y) = 0$. In the remaining cases, we can first establish and then use the identity $w = \mathbf{sgn}(w)|w|$ to complete the argument.

In all proofs by cases, ***it is important to be absolutely certain that ALL possibilities have been listed.*** The omission of some cases is an automatic mistake in any proof.

Interchanging roles of variables. This is a basic example of proofs by cases in which it is possible to "leverage" one case and obtain the other with little or no additional work.

Example. Show that if **x** and **y** have opposite signs, then we have $|x - y| = |x| + |y|$.

SOLUTION: Suppose first that **x** is positive and **y** is negative. Then the left hand side is just $x + |y| = |x| + |y|$. Now suppose **y** is positive and **x** is negative. Then if we apply the preceding argument to **y** and **x** rather than to **x** and **y** we then obtain the equation $|y - x| = |y| + |x|$. Since the left hand side is equal to $|x - y|$ and the right hand side is equal to $|x| + |y|$, we get the same conclusion as before. In a situation of this type we often say that *the second case follows from the first by reversing the roles of* **x** *and* **y**.

Vacuous proofs. In some instances a statement is true because there are no examples where the hypothesis is valid.

Example. Show that if **x** is a number such that $x + 1 = x$, then $x^2 + 1 = x^2$.

SOLUTION: There is no number satisfying the hypothesis, so whatever conclusion one states, there will be no number which satisfies the first but does not satisfy the second. Formally, the statement $P \Rightarrow Q$ merely signifies that there are no situations in which **P** is true but **Q** is false; if there are no situations where **P** is true, then there also cannot be any where **P** is true but **Q** is false.

How can this be useful in mathematics? Sometimes the use of vacuously true statements allows one to state conclusions in a simpler or more uniform manner. For example, in elementary geometry one can show that the sum of the measures of the vertex angles for a regular $n-$gon is equal to $180(n-2)/n$ degrees. Strictly speaking this is only valid if n is at least 3 because every regular polygon has at least three sides, but for some purposes it is convenient simply to state the formula for all positive integers n. The formula gives a negative angle measurement when $n = 1$, but in some sense this does not matter; the formula does not apply if $n = 1$ because there is no such thing

as a $1-$gon. The point is that the statement of the formula is logically correct even if we omit the condition that n is at least 3. This is a simple situation, but the concept of "vacuously true" also turns out to be useful in other situations where the hypothesis or conclusion is more complicated.

Adapting existing proofs. In all activities, it can be useful to use an idea that has worked to solve one problem in an attempt to solve another that may be somehow related. The same principle works for mathematical proofs. You can try this approach in order to prove that if $3x + 1 = 10$, then $x = 3$ (modify the first proof above).

Disproving conjectures. Frequently one is faced with an unproven statement and the goal is to determine whether it is true or false. If you suspect the statement is false, often the fastest and simplest way to confirm this is to construct a ***counterexample*** which satisfies the hypotheses but not the entire conclusion.

Illustration. If we are given real numbers a and b such that $a^3 - a = b^3 - b$, can we conclude that $a = b$?

SOLUTION: We should remark first that this is true if the absolute values of a and b are greater than 2, and someone who knows this might wonder if it is evidence that the result is always true. However, it is not; to show this we need to find explicit distinct values of a and b for which the equation holds. This can be done systematically, but the fastest way is to look at some examples and notices that the numbers 0 and 1 provide a counterexample.

On the other hand, ***it is important to recognize that one cannot prove a general statement by simply checking one, several, or even infinitely many examples that do not exhaust all the possibilities,*** and the preceding statement demonstrates this very convincingly (it is true whenever a and b are greater than 2).

Contrapositives, biconditionals and logical equivalences. In order to complete a proof of the biconditional (or logical equivalence) statement **P** $\Leftrightarrow$ **Q,** it suffices to prove the two separate statements **P** $\Rightarrow$ **Q** and (its "inverse" statement) **not P** $\Rightarrow$ **not Q.** **[**The reason for this rule is that the inverse statement **not P** $\Rightarrow$ **not Q** is the contrapositive of the converse statement **Q** $\Rightarrow$ **P.]**

Similarly, in order to complete a proof of **P** $\Leftrightarrow$ **Q,** it suffices to prove the contrapositive statement **not Q** $\Rightarrow$ **not P** and the inverse statement **not P** $\Rightarrow$ **not Q.**

Proofs of existence and uniqueness. It is *absolutely essential* to remember that ***all*** *such proofs have* ***two*** *parts*, one of which is an ***existence*** *proof* and the other of which is a ***uniqueness*** *proof.*

A symbolic approach to proofs. If it is difficult to decide how to start a proof, one suggestion is to put things into symbolic terms along the lines of the present section. This may provide enough insight into the question that a successful proof strategy can be found.

The use of definitions as a proof strategy. Another suggestion for finding a proof strategy is to recall all relevant definitions; it is very easy to overlook these or recall them inaccurately.

The do – something approach to finding proofs. This is simply trial and error, but it definitely should not be underestimated (recall Thomas Edison's comment about genius being 99 per cent perspiration and one per cent inspiration!). Even if no particular way of getting from the start to the finish is apparent, there is often little to lose by simply getting involved, doing something, trying different approaches, drawing pictures and proving everything that one can from the information given. Most of the proofs in print give no idea of the dead ends, incomplete arguments and otherwise unsuccessful efforts at proving something that took place before a valid proof was found. Trial and error is just as much a part of proofs in mathematics as it is of any other intellectual activity.

Mathematical induction (Finite induction). This is often a very powerful technique, but it is really more of a method to provide a formal verification of something that is suspected to be true rather than a tool for making intuitive discoveries, but it is absolutely essential. The use of mathematical induction dates back at least to some work of F. Maurolico (1494 – 1575). There are many situations in discrete mathematics where this method is absolutely essential; we shall postpone discussing this until Unit **V**.

Avoiding and finding mistakes in proofs. Unfortunately, there is no simple way of doing these outside of checking things repeatedly and carefully, but we have already mentioned a few common causes of difficulties and how to prevent them and there are several more common errors that can be mentioned: The list below is by no means exhaustive.

1. ***Begging the question.*** Frequently one finds arguments in which a proof uses and relies upon some other auxiliary which has not been proven. In such instances all one has shown is that *if this auxiliary statement is true, then the original statement is true*. However, we may have no way of knowing whether the auxiliary statement is true or false.
2. ***Computational errors.*** Sometimes mistakes in arithmetic or algebra are embedded in arguments and destroy their validity.
3. ***Incorrect citations of other results.*** Of course, this can be deadly to a proof. Division by zero is a standard elementary example, in which one neglects to recognize that **ax = ay** *implies* **x = y** *only if* **a** *is nonzero*.
4. ***Proving only half of biconditional or existence – uniqueness proofs.*** Half a proof may be better than none at all, but it is still just half a proof.
5. ***Proving the converse instead.*** Often one finds arguments which show that if the conclusion is true, then the hypothesis is true. This is the reverse of what is supposed to be established.
6. ***Using unproven converses.*** This is a special case of the third item, but it is also one which plays a role in elementary algebra.

The last of these is related to material on ***extraneous roots*** that one finds in elementary algebra courses. Here is a quick review of the underlying ideas. Suppose that we want to solve an equation like

$$x - 3 = \sqrt{30 - 2x}\,.$$

The standard way to attack this problem is to eliminate the radical by squaring both sides and solving for **x:**

$$(x-3)^2 = \left(\sqrt{30-2x}\right)^2$$
$$x^2 - 6x + 9 = 30 - 2x$$
$$x^2 - 4x - 21 = 0$$
$$(x-7)(x+3) = 0$$
$$x = 7; x = -3$$

(***Source:*** **http://regentsprep.org/Regents/mathb/7D3/radlesson.htm**)

This tells us that the only possible solutions are given by the two values above, but ***it does not guarantee that either is a solution.*** The reason for this is that the first step, in which we square both sides, shows that the first equation implies the second, but it does not imply that the second implies the first; for example, even though the squares of 2 and -2 are equal, it clearly does **not** follow that these two numbers are the same. In order to complete the solution of the problem, we need to go back and determine which, if any, of these two possible solutions will work. It turns out that $x = 7$ is a solution, but on the other hand $x = -3$ is not (and hence is an extraneous root).

The online site **http://www.jimloy.com/algebra/square.htm** discusses further examples of this type.

Pólya's suggestions for solving problems. The classic book, ***How to solve it,*** by G. Pólya (1887 – 1985), discusses useful strategies for working problems in mathematics. A summary of his suggestions and a more detailed reference for the book appear in the online document

http://math.ucr.edu/~res/polya.pdf

which is stored in the course directory.

Ends of proofs. In classical writings mathematicians used the initials **Q. E. D.** (for the Latin phrase, *that which was to be demonstrated*) or **Q. E. F.** (for the Latin phrase, *that which was to be constructed*) to indicate the end of a proof or construction. Some writers still use this notation, but more often the end of a proof or line of reasoning is now indicated by a large black square, which is sometimes known as a "tombstone" or "Halmos (big) dot." We shall also use the symbol "■" to mark the end of an argument.

Reference for further reading. There is an article on writing proofs ("A guide to proof – writing," by R. Morash) on pages 437 – 447 of the following supplement to Rosen's text:

K. Rosen, ***Student Solutions Guide to Discrete Mathematics and Its Applications*** (5th Ed.). McGraw – Hill, Boston, 2003. ISBN: 0–07–247477–7.

Of course, there are also many other excellent books available; we have chosen one that is closely related to a text that was consulted repeatedly in the preparation of these notes.

II.2 : Notation and first steps

(Halmos, § 1; Lipschutz, §§ 1.2 – 1.5, 1.10)

We shall start by summarizing the naïve approach, and then we shall explain how things can be set up more formally. A reader who wishes to skip the latter may do so by going directly from the end of the discussion of the former to the final portion of this section titled *A few simple consequences*.

The naïve approach

Most if not all of this is probably familiar, but it is necessary to state things explicitly for the sake of completeness.

In the mathematical sciences, a "***set***" is supposed to be a ***collection of objects***; as noted on page 4 of Halmos, "A pack of wolves, a bunch of grapes or a flock of pigeons are all examples." To illustrate the generality of the concept, we note that the objects in a set may themselves be sets. For mathematical purposes the only relevant information about a set concerns the objects belonging to it, and accordingly ***a set is completely determined by the objects that belong to (or are members of) it.*** If an object **x** belongs to a set **X**, we shall denote this fact by the usual notation $x \in X$.

There are two standard ways of describing a set. In some cases we can describe the set by ***listing*** all the objects in it. For example, the set consisting of the positive integers from 1 to 5 may be denoted by $\{1, 2, 3, 4, 5\}$. On the other hand, a set is often described in terms of the properties that are true for objects belonging to it and false for objects that do not belong to it. For example, if we wish to describe the set of whole numbers that are perfect squares, we use what is called ***set builder notation***:

$$\{ x \mid x \text{ is an integer and } x = y^2 \text{ for some integer } y \}$$

This is read verbally as "the set of all **x** such that **x** is an integer and **x** is equal to y^2 for some integer **y**" (where the vertical line "|" is read "such that").

The possibility of a set which has no members is generally allowed, and it is called the "***empty set***" (or ***null set***). It is generally denoted by symbolism such as $\emptyset$.

A "**subset**" of a set **X** is simply a set which contains some but not necessarily all of the objects in **X**, and it is a "**proper subset**" if it does not contain all of the objects in **X**.

Subsets are denoted using the symbol $\subset$, and the statement $Y \subset X$ is often expressed verbally as "**Y** *is a subset of* **X**" or "**Y** *is contained in* **X**" or "**X** *contains* **Y**." Sometimes we shall also express this relationship using the notation $Y \supset X$.

There is one further point which is usually omitted in elementary treatments of set theory but must be mentioned here. Although there is a great deal of flexibility in the sorts of properties that can be used to define a set, serious problems arise if one tries to stretch

this too far. Such difficulties were first discovered at the end of the 19th and beginning of the 20th century and involve collections that are somehow "too big" to be handled effectively. For example, problems arise if one tries to talk about "the set of all possible sets." Further information on this appears on pages 6 – 7 of Halmos and in the more formal approach to set theory in this section.

There are two ways of avoiding such problems with oversize collections. One is to recognize their existence but to have a two-tiered system of collections in which some are regarded as sets and others are not. The latter are generally too large, and one cannot do as much with them as one can with sets. For example, a collection which is not a set cannot be viewed as a member of some other collection. Fortunately, these exceptional objects do not cause any real problems most of the time; in nearly all situations, the foundational questions can be avoided by assuming that everything in sight lies inside some very large and fixed *quasi – universal* set.

Once again, a reader who wishes to skip the more formal discussion of the framework for set theory may do so by proceeding directly to the heading, *A few simple consequences*.

A more formal approach

> Nothing will come of nothing.
>
> (Shakespeare, ***King Lear,*** Act **I**, Sc. 1)
>
> We can't define anything precisely. If we attempt to, we get into that paralysis of thought that comes to philosophers **…** one saying to the other: "You don't know what you are talking about**!**" The second one says: "What do you mean by talking? What do you mean by you? What do you mean by know**?**"
>
> R. Feynman (1918 – 1988), ***The Feynman Lectures on Physics***

Every logical discussion must begin somewhere. An endless sequence of definitions or proofs based on earlier ones will not lead to any firm conclusions. In order to begin, the following three requirements must be fulfilled:

1. There must be a mutual understanding of the words and symbols to be used.
2. There must be acceptance of certain statements whose correctness is not further justified.
3. There must be agreement about the ***rules of reasoning*** which determine how and when one statement follows logically from another.

The words and symbols in the first item are generally known as ***undefined concepts*** in mathematics, and the statements described in the second item are generally known as ***assumptions, axioms*** or ***postulates*** (in modern usage all these are synonymous). We have already treated the rules of reasoning in Section **II.0.**

By modern standards, one logical difficulty with Euclid's ***Elements*** is that it tried to define everything. For example, a point was defined to be something that had no "part" or dimensions; to be logically precise, such a definition depends in turn upon giving a sound definition of "part" or dimension, and of course the same applies to any terms used in the definitions of the latter. The introduction of undefined concepts eliminates such infinite regressions. However, it is important to recognize that undefined concepts may not have any real value unless one has some understanding of what they are supposed to represent. In other words, if deductions are expected to yield useful information, then the undefined concepts in a discussion should be formal idealizations of things that are relatively familiar and recognizable.

Undefined concepts in set theory

Not surprisingly, the most important undefined concept in this subject is a set, which corresponds to a collection of objects. Since one important property of such a collection is whether some given object belongs to it, the notion of one entity belonging to another is almost as basic of an undefined concept as the notion of a set itself.

In order to avoid logical difficulties with oversized sets described above, we shall work with ***three*** primitive concepts which reflect the intuitive notions in the preceding paragraph.

1. ***CLASSES.*** These are collections of objects; it is assumed that each object itself is also a class.
2. ***SETS.*** Collections of objects that are small enough to work with reliably.
3. ***MEMBERSHIP.*** A grammatical statement with two subjects that represents one class belonging to another.

Items of the first type (actually, two types) are generally denoted by symbols such as letters. The statement that a class **A** belongs to a class **B** is usually written in the standard manner as $\mathbf{A} \in \mathbf{B}$. Likewise, we shall write $\mathbf{A} \notin \mathbf{B}$ to indicate that **A** does ***NOT*** belong to the class **B**. Following standard mathematical usage, we shall often use expressions of the following types as synonyms for $\mathbf{A} \in \mathbf{B}$:

- **A** belongs to **B.**
- **A** is a member of **B.**
- **A** is an element of **B.**

Furthermore, we shall often say that the *members* or *elements* of a class **B** are all the objects **A** such that $\mathbf{A} \in \mathbf{B}$. None of this is surprising, but the important point is that we are trying to build a theory of sets that is completely formal starting from scratch, and we need to start with this familiar sort of structure.

Comments on the introduction of classes as an undefined concept. Our approach, which differs from Halmos in that we also mention certain collections of objects that are too large to be treated as sets; this viewpoint was developed by J. von Neumann (1903 – 1957). As an example of the logical problems with an overly casual approach to set theory that are discussed in pages Halmos, we note that difficulties arise if one attempts to consider a ***universal set*** containing all sets. More will be said about this in the discussion of Russell's Paradox in Section **II.3.** The viewpoint of these notes

resembles the approach taken in many versions of axiomatic set theory**:** It ***is*** meaningful for us to talk about a universal collection or ***class*** of objects**,** but the latter is simply too large to be treated as a set**.** If a class is ***NOT*** a set**,** we shall say that it is a ***proper class.***

Our first basic assumption will be a smallness property that characterizes sets**.**

SMALLNESS PROPERTY FOR SETS. *A class* **A** *is a set if and only if* $\mathbf{A} \in \mathbf{B}$ *for some class* **B.**

Some good news. As we have already noted**,** in mathematics it is usually not necessary to worry very much about the formal distinction between sets and classes**.** The following paragraph summarizes the situation**:**

> For all practical purposes within this course**,** and nearly all other purposes in higher mathematics**,** one can simply view a set as a collection of objects that is not too large**;** a standard way of doing this is to ***assume that all objects in a given situation are subsets of some fixed larger set.***

The most significant exceptions to this principle arise in material dealing explicitly with the foundations of mathematics**.**

The definitions of *subclass* and *subset* are now straightforward**.**

Definition. Let **A** and **B** be classes of objects. We shall say that **A** is a ***subclass*** of **B** and write $\mathbf{A} \subset \mathbf{B}$ if for each object **x** such that $\mathbf{a} \in \mathbf{A}$**,** then we also have $\mathbf{x} \in \mathbf{B}$**.** If in addition **A** and **B** are sets**,** then we shall say that **A** is a ***subset*** of **B.**

If $\mathbf{A} \subset \mathbf{B}$ and the class **B** is small enough to be a set then one would expect the same holds for the class **A,** and in fact this is the case**.**

SUBSET PROPERTY. *If* $\mathbf{A} \subset \mathbf{B}$ *and* **B** *is a set, then* **A** *is also a set.*

Previous experience with set theory suggests that two sets should be the same if and only if they contain exactly the same objects**.** The next property reflects this basic fact**.**

EXTENSIONALITY PROPERTY. *If* **A** *and* **B** *are classes, then* $\mathbf{A} = \mathbf{B}$ *if and only if we have* $\mathbf{A} \subset \mathbf{B}$ *and* $\mathbf{B} \subset \mathbf{A}$**.**

Finally**,** we need to add another simple assumption**,** without which the whole theory would be entirely meaningless**.**

MINIMAL EXISTENCE PROPERTY. *There exists at least one set.*

A few simple consequences

Regardless of whether we adopt a naïve or more formal approach to set theory**,** there are already a few conclusions that can derived from what we have developed thus far**.** Here are two simple but important logical consequences of the definition of a subset or subclass**:**

Proposition 1. *For each class* **A** *we have* $\mathbf{A} \subset \mathbf{A}$**.**

Proof. By definition of subclasses, this amounts to saying that for all **x** such that **x** $\in$ **A,** we have **x** $\in$ **A.** But this follows because every true statement implies itself.■

Definition. If **A** and **B** are classes of objects such that **A** $\subset$ **B,** we shall say that **A** is a *proper subclass* of **B** if in addition **A** $\neq$ **B** (and a *proper subset* if **B** is a set).

Proposition 2. *If we are given classes* **A, B, C** *such that* **A** $\subset$ **B** *and* **B** $\subset$ **C,** *then we also have* **A** $\subset$ **C.**

Proof. By definition of subclasses and the assumptions, we know that for each **x** such that **x** $\in$ **A,** we also have **x** $\in$ **B.** Likewise, for each **y** such that **y** $\in$ **B,** we also have **y** $\in$ **C.** Combining these, we conclude that for each **x** such that **x** $\in$ **A,** we must also have **x** $\in$ **C.**■

The Extensionality Property (two classes are the same if they have the same elements) has a simple but fundamental consequence.

Proposition 3. *If* **A** *is a* ***proper*** *subclass of* **B,** *then there exists some object* **x** *such that* **x** $\in$ **B** *but* **x** $\notin$ **A.**

Proof. By hypothesis we know that **A** $\subset$ **B** but **A** $\neq$ **B.** If **B** $\subset$ **A** were true, then by extensionality we would have **A** = **B.** Therefore **B** $\subset$ **A** must be false, and this means that there must be some **x** such that **x** $\in$ **B** but **x** $\notin$ **A.**■

Variants of sets

For certain purposes it is useful to have elaborations of sets known as *multisets* (also called ***bags***) and *fuzzy sets*. For both of these, the extra data are numerical "values of membership" attached to each element. In the case of multisets, the value is a positive integer and it indicates that an element is somehow repeated; a simple example would be the roots of a quadratic equation, where one might have two single roots or one double root. For fuzzy sets, the value of membership is a real number in the unit interval, and intuitively it can be viewed as a probability that the element actually belongs to the set in question. Further discussions of both concepts are given on pages 96 – 97 of Rosen.

II.3 : Simple examples

(Halmos, §§ 1 – 3; Lipschutz, § 1.12)

Thus far the only specific example of a set we have mentioned is the empty set, and at this point we need some ways of constructing other examples. Once again, prior experience with set theory suggests that one can define a set by stipulating that the objects contained in it satisfy a given condition. Our next order of business is to make this more precise; the following version covers both the naïve and formal approaches.

SPECIFICATION PROPERTY. *Suppose that we are given a set* **A** *and an admissible predicate statement* **P(x).** *Then there is a subset* $\mathbf{B} \subset \mathbf{A}$ *such that* $\mathbf{x} \in \mathbf{B}$ *if and only if* $\mathbf{x} \in \mathbf{A}$ *and the statement* **P(x)** *is true.*

To elaborate on comments in the previous section, some standard ways of writing such a set are

$$\{ x \mid x \in A \,\&\, P(x) \} \quad \text{or} \quad \{ x \in A \mid P(x) \} \quad \text{or} \quad \{ x \in A : P(x) \}.$$

The admissibility requirement is included to guarantee that the statement **P(x)** is meaningful in our context; for most practical purposes it will create no problems. A brief discussion of suitably meaningful statements appears on pages 5 – 6 of Halmos.

It is possible to weaken the Specification Axiom somewhat to eliminate the dependence on some predetermined set **A,** but in practice this requirement is not an obstacle and the weaker statement is considerably more complicated to state. However, some additional condition is needed to avoid logical difficulties. We shall not give an explicit description of admissibility, but it is useful to discuss the problems which showed the need for such a restriction.

Admissible statements and Russell's Paradox

The most convincing example to illustrate the need to avoid totally unrestricted constructions of the form

$$\{ x \mid P(x) \}$$

was discovered by B. Russell (1872 – 1970; much better known outside of mathematics for his philosophical writings and political activism) near the beginning of the 20th century. He considered the simple example where **P(x)** is given by $x \notin x$. Suppose we can construct a set $A = \{ x \mid x \notin x \}$. One can then ask whether or not $A \in A$. If the answer is ***yes***, then the definition of **A** would seem to imply that $A \notin A$, while if the answer is ***no***, then the definition of **A** would seem to imply that $A \in A$. Each options leads to a contradiction, and hence neither is acceptable. Numerous other problems of a similar nature were discovered around the same time. Eventually it became clear that the underlying difficulty resulted from attempts to use sentences which somehow refer to themselves (think about the nonmathematical statements, "This sentence is false," or "No generalization is worth very much, including this one."). The specific condition in our Specification Axiom is a simple but effective way of doing so.

The idea of a set being an element of itself is somewhat contrary to our intuition, and in the usual forms of set theory in use today the possibility is excluded. We shall discuss this further in Section **III.4.**

A formal approach to the empty set

A reader who wishes to bypass material on the formal approach to set theory may skip this discussion and proceed directly to the next heading.

We have not yet explained how or why the empty set fits into our formal approach to set theory. The Specification Property gives us an easy way of doing so.

Proposition 1. *In the formal approach to set theory, there is a unique* ***empty set*** $\emptyset$ *with the property that* $x \notin \emptyset$ *for every set* x.

Proof. Since we just assumed the existence of a set, let us try to use this right away. Let A be a set, and use the Specification Axiom to construct the set

$$N = \{ x \in A \mid x \neq x \}.$$

For all $y \in A$ we have $y = y$ and therefore it follows that $y \notin N$ for all $y \in A$. By construction it follows that $z \notin N$ for all $z \notin A$, and therefore we conclude that $x \notin N$ for every set x. This proves the ***existence*** part of the proposition.

To prove ***uniqueness,*** let M and N be sets such that $x \notin M, N$ for every set x. Since nothing belongs to either set the statements $M \subset N$ and $N \subset M$ are vacuously true, and therefore by the Extensionality Property we must have $M = N$.■

Important special cases of the Specification Axiom

At least informally, the uses of the specification axiom to construct sets should be clear. For example, if we have a set $\mathbb{R}$ of real numbers with the expected properties then we can define the ***closed interval***

$$[0, 1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$$

and similar subsets that arise repeatedly in calculus and other mathematics courses. Our interest here will be more directed towards simple general constructions. The remainder of this section is valid for both the naïve and formal approaches.

Proposition 2. *Suppose that* A *is a set. Then there is a set* $\{A\}$ *such that* $A \in \{A\}$ *if and only if* $x = A$.

The set $\{A\}$ is sometimes called ***singleton*** A.

Proof. Since A is a set we know that $A \in B$ for some B. By the Specification Axiom there is a set given by the description $\{x \in B \mid x = A\}$. This is the set $\{A\}$ which is described in the conclusion.■

It is important to recognize the difference between A and $\{A\}$, particularly since it is very tempting and natural (but **dangerously incorrect!!**) to abbreviate the latter to A. As noted near the bottom of page 4 in Halmos,

> *A box that contains a hat and nothing else is not the same thing as a hat.*

The preceding result yields a simple example of a nonempty set.

Corollary 3. *There is a nonempty set* A *such that* $x \in A$ *if and only if* $x = \emptyset$.■

Since we are discussing results involving the empty set, this is a good time to mention one of its basic properties.

Proposition 4. *For every set* A *we have* $\emptyset \subset A$.

Proof. This is similar to the last paragraph of the preceding argument. Since nothing belongs to $\emptyset$ the statement "$(\forall x)\ x \in \emptyset \Rightarrow x \in A$" is vacuously true.■

Sets defined by finite lists

We would like to elaborate upon the argument in Proposition 2 to show that for each finite list of sets $A_1, \ldots, A_n$ there is a set $\{A_1, \ldots, A_n\}$ such that $B \in \{A_1, \ldots, A_n\}$ if and only if $B = A_k$ for some choice of k. In order to keep the discussion simple, we shall initially limit ourselves to the case where $n = 2$.

PAIRING PROPERTY. *If* **A** *and* **B** *are two sets, then there exists a third set* **C** *such that* $A \subset C$ *and* $B \subset C$.

Proposition 5. *Suppose that* **x** *and* **y** *are distinct sets. Then there is a set* $\{x, y\}$ *(the* ***unordered pair****) such that* $z \in \{x, y\}$ *if and only if* $z = x$ *or* $z = y$.

Proof. By the Pairing Axiom there is a set **C** such that $\{x\} \subset C$ *and* $\{y\} \subset C$. Therefore by the Specification Axiom there is a set defined by the description $\{z \in C \mid z = x \text{ or } z = y\}$. This is precisely the set described in the conclusion.■

In most situations that arise in mathematics, if we are given a finite list of sets $A_1, \ldots, A_n$ then the underlying assumptions will imply the existence of a set **C** such that $A_k \in C$ for all k, and in such cases there is a simple generalization of the previous result.

Proposition 6. *Suppose that* $A_1, \ldots, A_n$ *are sets, and assume also that there is some set* **C** *such that* $A_k \in C$ *for all* k. *Then there exists a set* $\{A_1, \ldots, A_n\}$ *such that we have* $B \in \{A_1, \ldots, A_n\}$ *if and only if* $B = A_k$ *for some* k.

Proof. In this case the desired set is given by the following condition:

$$\{x \in C \mid x = A_k \text{ for some } k\}$$

Equivalently, the set is also given by the following description:

$$\{x \in C \mid x = A_1 \text{ or } x = A_2 \text{ or } \ldots \text{ or } x = A_n\}$$

Either way we obtain the desired set.■

Further examples. The middle paragraph on page 10 of Halmos gives several examples of sets that can be constructed using the information about set theory that we have covered up to this point.

III : Elementary constructions on sets

In this unit we cover the some fundamental constructions of set theory that are used throughout the mathematical sciences.

Much of this material is probably extremely familiar, but we shall start at the beginning for several reasons, including the following:

1. To ensure that the discussion is complete.
2. To emphasize the more abstract perspective on the material.
3. To state some subtle but important differences in terminology between these notes and more elementary treatments of the material.

In the final section of this unit we shall indicate how one expresses everything in more formal and axiomatic terms.

Numbering conventions. In mathematics it is often necessary to use results that were previously established. Throughout these notes we shall refer to results from earlier sections by notation like Proposition **II.4.6,** which will denote Proposition **6** from Section **II.4** (this particular example does not actually exist, but it should illustrate the key points adequately).

III.1 : Boolean operations

(Halmos, §§ 4 – 5; Lipschutz, §§ 1.6 – 1.7)

We shall begin with a discussion of unions, intersections and complements. In order to keep the discussion simple and familiar at the beginning, we shall begin by considering only those sets which are subsets of some fixed set **S.**

Definitions. Let **A** and **B** be subsets of some set **S.** The standard ***Boolean operations*** on these sets are defined as follows:

- The ***intersection*** of **A** and **B** is the set of all elements common to both sets. It is symbolized by $A \cap B$ or $\{ x \in S \mid x \in A \text{ and } a \in B \}$.
- The ***union*** of two sets **A** and **B** is the set of elements which are in **A** or **B** or both. It is symbolized by $A \cup B$ or $\{ x \in S \mid x \in A \text{ or } x \in B \}$.
- The ***relative complement*** of **A** in **S** is the set of all elements in **S** that do not belong to **A.** It is symbolized by $S - A$ or $\{ x \in S \mid x \notin A \}$.

Numerous other symbols are also used for the relative complement of **A,** including

A′, A^c and also **A** with a long horizontal line over it ($\overline{A}$)**.**

We shall now review and prove the standard relationships between these three operations on subsets of **S.** The first group describes the algebraic identities involving unions and intersections which appear in the writings of G. Boole**.**

Theorem 1. *Let* **A, B** *and* **C** *be subsets of some fixed set* **S.** *Then the union and intersection defined as above satisfy the following* ***Boolean algebra*** *identities:*

(Idempotent Law for unions.) A ∪ A = A.

(Idempotent Law for intersections.) A ∩ A = A.

(Commutative Law for unions.) A ∪ B = B ∪ A.

(Commutative Law for intersections.) A ∩ B = B ∩ A.

(Associative Law for unions.) A ∪ (B ∪ C) = (A ∪ B) ∪ C.

(Associative Law for intersections.) A ∩ (B ∩ C) = (A ∩ B) ∩ C.

(Distributive Law 1.) A ∩ (B ∪ C) = (A ∩ B) ∪ (A ∩ C).

(Distributive Law 2.) A ∪ (B ∩ C) = (A ∪ B) ∩ (A ∪ C).

(Zero Law.) A ∪ Ø = A.

(Unit Law.) A ∩ S = A.

The second group of set – theoretic relations also involves complementation**.**

Theorem 2. *Let* **A** *and* **B** *be subsets of some fixed set* **S.** *Then the union, intersection and relative complement satisfy the following identities***:**

(Double negative Law.) (A′)′ = A.

(Complementation Law 1.) A ∪ A′ = S.

(Complementation Law 2.) A ∩ A′ = Ø.

(De Morgan's Law 1.) (A ∪ B)′ = A′ ∩ B′.

(De Morgan's Law 2.) (A ∩ B)′ = A′ ∪ B′.

Most if not all the verifications of these rules are fairly straightforward**,** and they essentially follow from the formulas for propositional calculus listed in Section **II.0.** We shall fill in the details atfter the next heading**.** Some identities are more obvious than others (in particular**,** the distributive laws and De Morgan's laws are probably less intuitive than the commutative and associative laws)**,** and in these cases we shall also give alternate arguments that are more detailed**.**

Boolean operations and subsets

There are simple but important characterizations of the relationship $\mathbf{A} \subset \mathbf{B}$ in terms of unions and intersections.

Theorem 3. *Let* **A** *and* **B** *be subsets of some fixed set* **S.** *Then the following are equivalent*:

(i) $\mathbf{A} \cup \mathbf{B} = \mathbf{B}$

(ii) $\mathbf{A} \subset \mathbf{B}$

(iii) $\mathbf{A} \cap \mathbf{B} = \mathbf{A}$

Proof. There are four parts to the argument.

(i) $\Rightarrow$ (ii) If $\mathbf{x} \in \mathbf{A}$, then $\mathbf{x} \in \mathbf{A}$ or $\mathbf{x} \in \mathbf{B}$, and hence $\mathbf{x} \in \mathbf{A} \cup \mathbf{B}$, which is **B.** Hence we have $\mathbf{A} \subset \mathbf{B}$.

(ii) $\Rightarrow$ (i) If $\mathbf{A} \subset \mathbf{B}$ and $\mathbf{x} \in \mathbf{A} \cup \mathbf{B}$, then $\mathbf{x} \in \mathbf{A}$ or $\mathbf{x} \in \mathbf{B}$, and in either case we have $\mathbf{x} \in \mathbf{B}$. Hence we have $\mathbf{A} \cup \mathbf{B} \subset \mathbf{B}$. Conversely, if $\mathbf{x} \in \mathbf{B}$, then we must have $\mathbf{x} \in \mathbf{A}$ or $\mathbf{x} \in \mathbf{B}$, so that $\mathbf{B} \subset \mathbf{A} \cup \mathbf{B}$. Combining these, we have $\mathbf{A} \cup \mathbf{B} = \mathbf{B}$.

(ii) $\Rightarrow$ (iii) If $\mathbf{A} \subset \mathbf{B}$ and $\mathbf{x} \in \mathbf{A}$, then $\mathbf{x} \in \mathbf{B}$ and hence $\mathbf{x} \in \mathbf{A} \cap \mathbf{B}$, so that we have $\mathbf{A} \subset \mathbf{A} \cap \mathbf{B}$. Conversely, if $\mathbf{x} \in \mathbf{A} \cap \mathbf{B}$, then $\mathbf{x} \in \mathbf{A}$ and $\mathbf{x} \in \mathbf{B}$, and the latter means that $\mathbf{A} \cap \mathbf{B} \subset \mathbf{A}$. Combining these, we have $\mathbf{A} \cap \mathbf{B} = \mathbf{A}$.

(iii) $\Rightarrow$ (ii) If $\mathbf{x} \in \mathbf{A}$, then $\mathbf{A} \cap \mathbf{B} = \mathbf{A}$ implies that $\mathbf{x} \in \mathbf{A}$ and $\mathbf{x} \in \mathbf{B}$, and the second of these means we must have $\mathbf{A} \subset \mathbf{B}$.■

Verifications of the standard identities

We shall derive the identities of Theorems 1 and 2 roughly in the order they were stated.

Idempotent laws. The law for unions is true because $\mathbf{x} \in \mathbf{A} \Leftrightarrow \mathbf{x} \in \mathbf{A}$ or $\mathbf{x} \in \mathbf{A}$, while the law for intersections is true because $\mathbf{x} \in \mathbf{A} \Leftrightarrow \mathbf{x} \in \mathbf{A}$ and $\mathbf{x} \in \mathbf{A}$.

Commutative laws. The law for unions is true because

$$\mathbf{x} \in \mathbf{A} \cup \mathbf{B} \Leftrightarrow \mathbf{x} \in \mathbf{A} \text{ or } \mathbf{x} \in \mathbf{B} \Leftrightarrow \mathbf{x} \in \mathbf{B} \text{ or } \mathbf{x} \in \mathbf{A} \Leftrightarrow \mathbf{x} \in \mathbf{B} \cup \mathbf{A}$$

while the law for intersections is true because

$$\mathbf{x} \in \mathbf{A} \cap \mathbf{B} \Leftrightarrow \mathbf{x} \in \mathbf{A} \text{ and } \mathbf{x} \in \mathbf{B} \Leftrightarrow \mathbf{x} \in \mathbf{B} \text{ and } \mathbf{x} \in \mathbf{A} \Leftrightarrow \mathbf{x} \in \mathbf{B} \cap \mathbf{A}.$$

In symbolic terms, the preceding arguments are just special cases of the more general propositional equivalences

$$\mathbf{P} \vee \mathbf{Q} \Leftrightarrow \mathbf{Q} \vee \mathbf{P} \quad \text{and} \quad \mathbf{P} \wedge \mathbf{Q} \Leftrightarrow \mathbf{Q} \wedge \mathbf{P}$$

and we shall use other such equivalences freely in deriving the remaining assertions in the theorem.

Associative laws. The argument is similar, depending upon the general propositional equivalences

[P ∧ (Q ∧ R)] ⇔ [(P ∧ Q) ∧ R] and **[P ∨ (Q ∨ R)] ⇔ [(P ∨ Q) ∨ R]**

where **P, Q** and **R** are the statements **x ∈ A, x ∈ B** and **x ∈ C** respectively**.**

Distributive laws. The argument is again similar, depending upon the general propositional equivalences

[P ∧ (Q ∨ R)] ⇔ [(P ∧ Q) ∨ (P ∧ R)] and **[P ∨ (Q ∧ R)] ⇔ [(P ∨ Q) ∧ (P ∨ R)]**

where **P, Q** and **R** are the statements **x ∈ A, x ∈ B** and **x ∈ C** respectively.

Zero law. One can characterize the empty set as the set of all **x** such that **x ≠ x.** Thus we have **x ∈ A ∪ Ø ⇔ x ∈ A** or **x ≠ x,** and since the statement **x ≠ x** is always false the second condition is equivalent to **x ∈ A.**

Unit law. By hypothesis we know that **A** is a subset of **S** and therefore if **x ∈ A** we also have **x ∈ S,** so that **x ∈ A ∩ S.** Conversely**,** if **x ∈ A ∩ S** then we automatically have **x ∈ A.**

AN ALTERNATE APPROACH TO THE DISTRIBUTIVE LAWS. Here is a method for deriving the distributive laws that does not use abstract propositional equivalences**.** We include it because the equivalences in this case may be less transparent than the previous ones**.** Given **x ∈ S,** we know that *each one of the three fundamental statements* **x ∈ A, x ∈ B** *and* **x ∈ C** *is either* **true** *or* **false.** Thus there are exactly eight possibilities for every element of **S.** It will suffice to show that in each of these cases that if **x ∈ A ∩ (B ∪ C)** then **x ∈ (A ∩ B) ∪ (A ∩ C)** and conversely (this will prove the first distributive law)**,** and similarly if we have **x ∈ A ∪ (B ∩ C)** then **x ∈ (A ∪ B) ∩ (A ∪ C)** and conversely (this will prove the second distributive law)**.** The first step is to compile a table containing all eight possibilities**;** in the table below**,** + indicates that the relevant statement is true and **0** indicates that it is false**.**

x ∈ A	x ∈ B	x ∈ C
0	0	0
0	0	+
0	+	0
0	+	+
+	0	0
+	0	+
+	+	0
+	+	+

Note that if we replace + by **1** then these possibilities are an ordered list corresponding to the base two expansions of the integers **0** through **7.** Our next step is to add two columns to this table**,** one of which indicates whether **x ∈ A ∩ (B ∪ C)** in the given case and the other of which gives reasons for this conclusion**.**

$x \in A$	$x \in B$	$x \in C$	$x \in A \cap (B \cup C)$	*Reason(s)*
0	0	0	0	$x \notin A$
0	0	+	0	$x \notin A$
0	+	0	0	$x \notin A$
0	+	+	0	$x \notin A$
+	0	0	0	$x \notin B \cup C$
+	0	+	+	$x \in A$ & $x \in C$
+	+	0	+	$x \in A$ & $x \in B$
+	+	+	+	$x \in A$ & $x \in B$

We next carry out the same process for $x \in (A \cap B) \cup (A \cap C)$:

$x \in A$	$x \in B$	$x \in C$	$x \in (A \cap B) \cup (A \cap C)$	*Reason(s)*
0	0	0	0	$x \notin A$
0	0	+	0	$x \notin A$
0	+	0	0	$x \notin A$
0	+	+	0	$x \notin A$
+	0	0	0	$x \notin B \cup C$
+	0	+	+	$x \in A$ & $x \in C$
+	+	0	+	$x \in A$ & $x \in B$
+	+	+	+	$x \in A$ & $x \in B$

In both instances we see that **x** belongs to the set under consideration if and only if one of the last three possibilities is true**.** Therefore the two sets**,** namely $A \cap (B \cup C)$ and $(A \cap B) \cup (A \cap C)$**,** must be equal**.** This proves the first distributive law**.**

Of course, it is possible to approach the second distributive law similarly. We shall not carry out the details here (the latter is left to the reader as an exercise), but we note that $x \in S$ belongs to the sets under consideration in this situation if and only if one of the last five possibilities in the first table is true**.**■

This completes the discussion of Theorem 1**,** so we shall proceed to the identities in Theorem 2 involvling complementation**.**

Double negative law. Let **P** be the statement that $x \in A$**,** and let **Q** be the statement that $x \in S$**.** Since **A** is a subset of **S** we know that **P** is equivalent to $P \wedge Q$**.** The

statement $x \in A'$ is then given by $Q \wedge (\neg P)$, and the statement $x \in (A')'$ is then given by $Q \wedge \neg [Q \wedge (\neg P)]$. We then have the chain of logical equivalences

$$Q \wedge \neg [Q \wedge (\neg P)] \iff Q \wedge [(\neg Q) \vee (\neg \neg P)]$$

$$Q \wedge [(\neg Q) \vee (\neg \neg P)] \iff Q \wedge [(\neg Q) \vee P]$$

$$Q \wedge [(\neg Q) \vee P] \iff [Q \wedge (\neg Q)] \vee [Q \wedge P]$$

$$[Q \wedge (\neg Q)] \vee [Q \wedge P] \iff Q \wedge P \iff P$$

which show that $x \in (A')' \iff x \in A$.

Here is a nonsymbolic approach: In this case the two possibilities are given by the statements $x \in A$ and $x \notin A$. In the first case we know that $x \in A$ implies $x \notin A'$, which in turn implies that $x \notin (A')'$ is false or equivalently that $x \in (A')'$ is true. To prove the converse direction, note that $x \in (A')'$ implies $x \notin A'$, which we know is equivalent to $x \in A$. This completes the argument in the first case. In the second case, we know that $x \notin A$ implies $x \in A'$, which in turn implies $x \notin (A')'$. Conversely, if the latter is true then $x \in A'$, which in turn is equivalent to $x \notin A$. Thus in all cases we see that $x \in (A')' \iff x \in A$.

Complementation laws. If either $x \in A$ or $x \in A'$ then we also have $x \in S$, so that $A \cup A'$ is contained in S. Conversely, if $x \in S$, then we either have $x \in A$ or else we have $x \notin A$, or equivalently $x \in A'$, so that $x \in A \cup A'$. Therefore $A \cup A' = S$. Next, if both $x \in A$ and $x \in A'$ then we have $x \in A$ and $x \notin A$, which is impossible. Therefore there cannot be any x in the intersection and hence it must be empty.

De Morgan's laws. Let P and Q be the statements $x \in A$ and $x \in B$, and let R be the statement $x \in S$. The statement $x \in (A \cup B)'$ is then given by $R \wedge [\neg (P \vee Q)]$, and we can then chase the string of equivalences

$$R \wedge [\neg (P \vee Q)] \iff R \wedge (\neg P \wedge \neg Q)$$

$$R \wedge (\neg P \wedge \neg Q) \iff (R \wedge \neg P) \wedge (R \wedge \neg Q)$$

to see that $x \in (A \cup B)' \iff x \in A' \cap B'$. Likewise, the statement $x \in (A \cap B)'$ is given by $R \wedge [\neg (P \wedge Q)]$, and we can then chase the string of equivalences

$$R \wedge [\neg (P \wedge Q)] \iff R \wedge (\neg P \vee \neg Q)$$

$$R \wedge (\neg P \vee \neg Q) \iff (R \wedge \neg P) \vee (R \wedge \neg Q)$$

to see that $x \in (A \cap B)' \iff x \in A' \cup B'$.

Once again we shall give another proof of this without using propositional equivalences by breaking things down into cases. Here there are four possibilities, depending on whether each of the basic statements $x \in A$ and $x \in B$ is true. To save space we shall proceed directly to determine whether or not $x \in (A \cap B)'$ in the respective cases.

$x \in A$	$x \in B$	$x \in (A \cap B)'$	*Reason(s)*
0	0	+	$x \notin A$ & $x \notin B$
0	+	+	$x \notin A$
+	0	+	$x \notin B$
+	+	0	$x \in A$ & $x \in B$

If one carries out the analogous procedure with $x \in A' \cup B'$ replacing the third column, exactly the same result is obtained (with the same reasons in each case). Therefore, each of the separate statements $x \in (A \cap B)'$ and $x \in A' \cup B'$ holds in the first three of the four possibilities, and accordingly the two sets under consideration must be equal. This proves the second of De Morgan's Laws.

A similar approach yields the first of De Morgan's Laws; in this situation $x \in S$ belongs to the sets under consideration, which are $(A \cup B)'$ and $A' \cap B'$, in only the first of the four possibilities.■

III.2 : Ordered pairs and products

(Halmos, §§ 3, 6; Lipschutz, §§ 3.1 – 3.2)

We shall introduce ordered pairs axiomatically, following an approach outlined on page 25 of Halmos (see the paragraph beginning near the middle of the page). As shown the preceding discussion on pages 23 – 24 of Halmos, it is possible to derive our axiom(s) as consequences of the other assumptions introduced up to this point. There will be further discussion of efficient and irredundant systems of axioms later in these notes.

EXISTENCE OF ORDERED PAIRS. *Given two set-theoretic objects* **a** *and* **b,** *there is a set-theoretic construction which yields an*

ordered pair **(a, b)**

which has the fundamental property

(a, b) = (c, d) *if and only if* **a = c** *and* **b = d.**

Given two classes **A** and **B,** the ***Cartesian product*** $A \times B$ is defined to be the collection of all ordered pairs **(a, b)** where $a \in A$ and $b \in B$. This collection is also called the ***direct product*** of the two sets **A** and **B.**

Nonmathematical example. If set **V** is the set of playing card values **{ A, K, Q, J,** 10**,** 9**,** 8**,** 7**,** 6**,** 5**,** 4**,** 3**,** 2 **}** and set **S** is the set of playing card suits **{** ♠**,** ♥**,** ♦**,** ♣ **},** then the Cartesian product $V \times S$ corresponds to the standard deck of 52 playing cards:

$$\{ (A, \spadesuit), (K, \spadesuit), ..., (2, \spadesuit), (A, \heartsuit), ..., (3, \clubsuit), (2, \clubsuit) \}$$

Historical remarks. Clearly the name ***Cartesian product*** is an allusion to the well known work of R. Descartes (1596 – 1650) on introducing algebraic coordinates into geometry. This usage is somewhat ironic because Descartes himself did not explicitly use ordered pairs of numbers to represent points in his writings on coordinate geometry. The latter are formally just part of one addendum, *La Géométrie,* to his major work, *Discours de la méthode pour bien conduire sa raison et chercher la vérité dans les sciences* (Discourse on the Method of Correctly Reasoning and Seeking Truth in the Sciences). However, the name ***Cartesian product*** has stuck and is now unlikely to be changed. A detailed discussion about exactly how Descartes and several others, including P. de Fermat (1601 – 1665), introduced coordinates into geometry during the 17th century, and the significance of various individuals' contributions, is far beyond the scope of these notes, but some information on these topics is given on pages 370 and 375 – 376 of Burton, and the following references on the history of mathematics provide still more details:

> C. B. Boyer, ***A History of Mathematics.*** (Revised reprinting of the second edition, with a foreword by Isaac Asimov. Revised and with a preface by U. C. Merzbach.) *John Wiley & Sons, Inc., New York,* 1991. ISBN: 0–471–54397–7. [See in particular pages 345 – 346.]
>
> C. B. Boyer, ***History of Analytic Geometry.*** *Dover Publications, New York,* 2004. ISBN: 0–486–43832–5.
>
> M. Kline, ***Mathematical Thought from Ancient to Modern Times.*** Oxford University Press, Oxford, UK, 1972. ISBN: 0–195–01496–0.

In order to work effectively with Cartesian products like $\mathbf{A \times B}$ we need the following axiom.

CARTESIAN PRODUCT PROPERTY. *If* **A** *and* **B** *are sets, then so is* $\mathbf{A \times B}$.

If one uses the construction for ordered pairs on pages 23 – 24 of Halmos, then this axiom follows immediately (see the discussion on page 24).

In our setting (and the development in Halmos) it follows immediately that if **C** and **D** are subsets of **A** and **B** respectively, then $\mathbf{C \times D}$ is a subset of $\mathbf{A \times B}$ (compare the final sentence on page 25 of Halmos).

It is important to recognize that the products $\mathbf{B \times A}$ and $\mathbf{A \times B}$ are not necessarily equal. In fact, we have the following result:

Proposition 1. *If* **A** *and* **B** *are nonempty sets, then we have* $\mathbf{B \times A = A \times B}$ *if and only if* $\mathbf{A = B}$.

Proof. If $\mathbf{A = B}$ then we trivially have $\mathbf{A \times B = A \times A = B \times A}$. Conversely, suppose we have $\mathbf{B \times A = A \times B}$. Let $\mathbf{b \in B}$. Then for each $\mathbf{x \in A}$ we have $\mathbf{(b, x) \in B \times A = A \times B}$, which means that $\mathbf{b \in A}$. Thus we have shown that **B** is contained in **A**. Similarly, let $\mathbf{a \in A}$. Then for each $\mathbf{y \in B}$ we have $\mathbf{(y, a) \in B \times A = A \times B}$, which

means that $a \in B$. Thus we have shown that **A** is contained in **B.** Combining these, we conclude that $A = B$.■

Here is another elementary result on Cartesian products. The proof is left to the reader as an exercise.

Proposition 2. *If* **a** *and* **b** *are sets, then* $\{ a \} \times \{ b \} = \{ (a, b) \}$.■

A few simple formal identities involving Cartesian products, unions, intersections and complements are listed at the bottom of page 25 in Halmos, and more are given in the exercises for this section.

Notational remark. As noted on page 13 of the book by Munkres, the notation **(a, b)** for an ordered pair has an entirely different meaning than the use of **(a, b)** to denote an open interval in the real numbers; ***i.e.***, all real numbers **x** such that $a < x < b$. Usually it is very clear from the context which meaning should be given to **(a, b)** but there are some exceptions. The terminology $a \times b$ is sometimes used (for example, in Munkres), but this can also lead to conflicts of various sorts so we shall avoid it.

III.3 : Larger constructions

(Halmos, §§ 3, 5 – 6, 9; Lipschutz, §§ 1.9, 3.1 – 3.2, 5.1 – 5.2)

Usually the sets constructed in the preceding two sections are not much larger than the objects from which they are constructed. In this section we shall discuss some basic constructions which generally yield much larger examples.

Power sets

In Section **II.1** we noted that sets may themselves be elements of other sets. The following quoted passage from page 11 of Munkres, ***Topology*** (full citation below), explains the main idea in nonmathematical terms.

> *The objects belonging to a set may be of any sort. One can consider ... the set of all decks of playing cards in the world ...* [*which*] *illustrates a point we have not yet mentioned*; *namely, the objects belonging to a set may* ***themselves*** *be sets. For a deck of cards is itself a set, one consisting of pieces ...* [*and*] *the set of all decks of cares in the world is thus a set whose elements themselves are sets.*
>
> **[** ***Source:*** J. R. Munkres, ***Topology*** (Second Edition). Prentice – Hall, Upper Saddle River, NJ, 2000. ISBN: 0 – 13 – 18129 – 2.**]**

We may state this principle more formally as follows:

POWER SET PROPERTY. *If* **S** *is a set, then the collection* **P(S)** *of all subsets of* **S** *is also a set.*

This set of all subsets is often called the ***power set*** for reasons that will be explained in the next unit.

Note that union, intersection and complementation define algebraic operations on **P(S)** which satisfy the identities described above. In some ways union and addition behave like addition and multiplication, but a check of the Boolean algebra identities also shows some important differences (for example, the idempotent laws and the fact that one has an extra distributive law).

Examples. If **S** is the set **{1, 2, 3 }** then there are precisely **8 = 2^3** subsets in **P(S),** and they are all listed below:

Ø, {1}, {2}, {3}, {1, 2 }, {1, 3 }, {2, 3 }, {1, 2, 3 }

If **T** is the set **{1, 2, 3, 4 }** then there are precisely **16 = 2^4** subsets in **P(S),** and they may be obtained from the list above by **(*i*)** taking the eight sets in this list, **(*i i*)** adding the element **4** to each of the eight sets in this list. Clearly one could continue in this fashion to list the subsets of **{1, 2, 3, 4, 5 }** and even larger finite sets; in particular, the set of all subsets of **{1, … , n }** contains **2^n** elements.

Note that the power set construction can be iterated, yielding sets such as **P(P(S))**, **P(P(P(S)))**, and so forth.

Example. If **S** is the set **{1}** then **P(P(S))** consists of the objects **Ø**, **{ Ø }** , **{{1}}** , and **P(S)** .

Larger unions and intersections

We have already noted that the importance of set theory is directly tied to its usefulness in studying infinite collections of objects. In particular, it is often necessary to consider unions and intersections of more than two sets at a time. Therefore we shall need an axiom to guarantee that reasonable infinite unions and intersections will determine sets.

AXIOM OF UNIONS. *If* **A** *is a set and* **$(A)** *is the collection of all* **x** *such that* **x ∈ B** *for some* **B ∈ A**, *then* **$(A)** *is also a set.*

Nonmathematical example. If **A** represents the set of all decks of playing cards as above, then **$(A)** is just the set of all cards belonging to these decks.

Normally one writes **$(A)** in another notation that is more suggestive of taking unions; for example, we frequently use expressions like **$\cup$ {B | B ∈ A }** or **$\cup_{B \in A}$ B.** This set is often called the ***union*** of all the sets **B** in the collection **A.** Our choice of the symbol **$** is motivated by typographical limitations in the word processing program used to create these notes.

There is also a corresponding notion of intersection.

Proposition 1. *If* **A** *is a* ***nonempty*** *set then there is a set*

$$\{ x \in \$(A) \mid x \in B \text{ for } \underline{\textbf{all}}\ B \in A \}$$

which is called the ***intersection*** *of all the sets* **B** *in the collection* **A** *and written in the forms* $\cap \{B \mid B \in A\}$ *or* $\cap_{B \in A} B$.

This result is an immediate consequence of the Axiom of Specification. The reasons for assuming **A** is nonempty are discussed on pages 18 – 19 of Halmos; for most purposes it is simply enough to understand that there are some annoying (but not serious) logical complications if we allow the possibility $A = \emptyset$.■

Further topics involving large unions and intersections will be covered in Section **VII.1.**

Unions and intersections over subfamilies

The following result describes what happens to unions and intersections of families of sets if one passes from a family **F** to a subfamily **G** such that $G \subset F$.

Theorem 2. *Let* **F** *be a family of sets, and let* **G** *be a subfamily of* **F.** *Then we have*

$$\cup \{B \mid B \in G\} \subset \cup \{B \mid B \in F\}.$$

Furthermore, if **F** and **G** are nonempty then we also have

$$\cap \{B \mid B \in F\} \subset \cap \{B \mid B \in G\}.$$

Proof. Suppose that $x \in B_0$ for some $B_0 \in G$. Then we also know that $B_0 \in F$, and therefore **x** must also belong to $\cup \{B \mid B \in F\}$. Suppose now that **F** and **G** are nonempty and that $x \in \cap \{B \mid B \in F\}$. If $C \in G$, then $C \in F$, and therefore if $x \in B$ for every $B \in F$ then certainly $x \in B$ for every $B \in G$. If follows that $\cap \{B \mid B \in F\}$ is contained in $\cap \{B \mid B \in G\}$.

Products of more than two sets

We have already described the product of two sets in terms of ordered pairs. More generally, one can also discuss ordered **n** – tuples of the form $(x_1, \ldots, x_n)$ and define an **n** – fold Cartesian product $A_1 \times \ldots \times A_n$ which will be the collection of all ordered **n** – tuples $(x_1, \ldots, x_n)$ such that $x_k \in A_k$ for all **k** between **1** and **n**. There will be a few references to such constructions in the next few units, and in Section **V.1** of these notes we shall show that one can even construct Cartesian products of infinite lists of sets. We shall state the explicit generalizations from ordered pairs to ordered **n** – tuples below. Everything is a straightforward extension of the previous discussion for $n = 2$.

EXISTENCE OF ORDERED n – TUPLES. *Let* **n** *be a positive integer. Given a sequence of* **n** *set – theoretic objects* $a_1, \ldots, a_n$ *there is a set-theoretic construction which yields an*

$$\underline{\textit{ordered}}\ \textbf{n} - \underline{\textit{tuple}}\ \ (a_1, \ldots, a_n)$$

which has the fundamental property

$$(a_1, \dots, a_n) = (b_1, \dots, b_n) \text{ if and only if } a_i = b_i \text{ for all } i.$$

Given **n** classes $A_1, \dots, A_n$ the ***Cartesian product*** $A_1 \times \dots \times A_n$ is defined to be the collection of all ordered **n** – tuples $(a_1, \dots, a_n)$ where $a_i \in A_i$ for all **i.** This collection is also called the ***direct product*** of the classes**.**

GENERALIZED CARTESIAN PRODUCT PROPERTY. *If* $A_1, \dots, A_n$ *are sets, then so is* $A_1 \times \dots \times A_n$**.**

Here is an important special case**:**

Proposition 3. *If* $a_1, \dots, a_n$ *are sets, then* $\{a_1\} \times \dots \times \{a_n\} = \{(a_1, \dots, a_n)\}$**.**■

III.4 : A convenient assumption

(Halmos, § 2; Lipschutz, § 1.12)

In Unit **II,** the following question arose in connection with Russell's paradox**:**

Is it possible to have an object **z** *in set theory such that* $z \in z$**?**

We might not expect something like this to happen when we discuss collections of ordinary objects**,** but nothing that we have said thus far eliminates such possibilities from set theory**.** The purpose of this section is to note that the latter do not arise in the most widely used approaches to set theory and to explain how this is done**,** mainly from the naïve point of view**.**

There are also many questions of a similar nature that can be formulated**.** Here is one crucial example**:**

Is it possible to have objects **u** *and* **v** *such that* $u \in v$ *and* $v \in u$**?**

These and other questions were considered early in the 20th century**,** and the key general observation was first noticed by D. Mirimanov (1861 – 1945) in 1917**.** The following equivalent formulation was given by J. von Neumann in the 1920s**.**

AXIOM OF FOUNDATION. *For each nonempty set* **x** *there is a set* **y** *such that* $y \in x$ *and* $y \cap x = \emptyset$**.**

This assumption**,** which is also known as the **AXIOM OF REGULARITY,** can be rephrased entirely in terms of words as follows**:**

Every nonempty set is disjoint from ***at least one*** *of its elements.*

The relation between this axiom and the condition in Russell's paradox is contained in the following result**.**

Proposition 1. *For every set* z *we have* $z \notin z$.

Proof. Let x be the set $\{ z \}$, so that the Axiom of Foundation implies the existence of some y such that $y \in x$ and $y \cap x = \emptyset$. Since x contains only the element z, it follows that y must be equal to z, and thus the condition $y \cap x = \emptyset$ translates to the condition $z \cap \{ z \} = \emptyset$. The latter is in turn equivalent to $z \notin z$.■

Similarly, we can use the Axiom of Foundation to show that the answer to the second question is also ***NO***.

Proposition 2. *If* z *and* w *are sets, then either* $z \notin w$ *or* $w \notin z$ *is true (and both might be true).*

Proof. It will suffice to show that if $z \in w$ then $w \notin z$; therefore we shall suppose that $z \in w$ is true. Let x be the set $\{ z, w \}$, so that the Axiom of Foundation implies the existence of some y such that $y \in x$ and $y \cap x = \emptyset$. It follows immediately that either $y = z$ or $y = w$. If $y = z$, then $z \in w$ would imply that y and x have z in common, which contradicts the fundamental condition on y, so we must have $z \notin w$. Likewise, if $y = w$, then $w \in z$ would imply that y and x have w in common, which contradicts the fundamental condition on y, so we must have $w \notin z$. Therefore in all cases at least one of the statements $z \notin w$ or $w \notin z$ must be true.■

More general consequences along these lines are discussed and proved on pages 95 – 96 of the book by Goldrei (see the beginning of Unit **I** for full bibliographic information). We shall merely state Mirimanov's original formulation of the property and one generalization (both without proofs; see pages 95 – 96 of Goldrei for details):

Mirimanov's Axiom of Foundation. *There are no sequences of sets* $A_1, A_2, A_3, \ldots$ *such that* $A_k \in A_{k+1}$ *for all* k.

Special case. *There are no sequences of sets* $A_1, A_2, \ldots A_n$ *such that* $A_k \in A_{k+1}$ *for all* k *and* $A_n \in A_1$ *(i.e., there are* ***no finite length*** $\in$ ***– cycles****).*

The second statement follows from the first by reductio ad absurdum, for if a finite sequence of the described type existed, then one could extend it to an infinite sequence as follows: Given an arbitrary positive integer m, use long divising to write $m = qn + r$ where $0 \leq r < n$, and set $A_m = A_r$. By construction this is a ***periodic*** or ***repeating*** sequence such that $A_m = A_{m+n}$ for all m.■

FOOTNOTE. Biographical information on D. Mirimanov (also spelled Mirimanoff) is available at the following online site:

http://www.numbertheory.org/obituaries/OTHERS/mirimanoff.html

(Unfortunately, the chronology for his life is in French, but the main items in it should be decipherable, and standard Internet translation software should work reasonably well for this material.)

Should one really assume the Axiom of Foundation?

A few mathematicians have varying degrees of reservations about assuming the Axiom of Foundation**,** but most accept it both because **(1)** as we have noted it is convenient to do so**, (2)** the introduction of this assumption does not lead to any logical contradictions by itself**.** The second point requires some explanation**.** Later in these notes we shall discuss the following important question**:**

Can we be certain that our logical framework for mathematics is entirely free of contradictions?

Unfortunately, the answer is ***NO*****,** and in fact the answer is no for any system that involves infinite objects like the basic number systems such as the positive integers or the real numbers**.** However**,** if there is a logical contradiction in the standard framework for mathematics which includes the Axiom of Foundation**,** then fundamental results of K. Gödel (1906 – 1978) imply that there is already a logical contradiction in the framework if one drops this assumption**.** Further information on this and related topics will appear in Unit **VII** when we introduce the Axiom of Choice**.**

Here are some online references for approaches to set theory that do not assume the Axiom of Foundation**:**

http://en.wikipedia.org/wiki/Non-well-founded_set_theory

http://en.wikipedia.org/wiki/Axiomatic_set_theory

A more extensive (and quite advanced) reference for set theory without the Axiom of Foundation is *Non – well – founded sets***,** by P. Aczel**,** which is available at the following online site**:**

http://standish.stanford.edu/pdf/00000056.pdf

Historical remarks

With the emergence of Russell's paradox, most mathematicians and logicians from that time concluded that set theory probably should not contain objects for which $x \in x$ or pairs of objects such that $x \in y$ and $y \in x$**.** Russell's approach to eliminating such phenomena was to introduce a ***theory of types*****,** in which sets have well – defined ***types*** or ***levels*** such that the level a set should exceed the level of its elements**.** Such a theory will not contain objects with the undesirable properties described above**,** and it also will not allow the other sorts of paradoxes that arose near the beginning of the 20th century. The theory of types played a central role in Russell's work with A. N. Whitehead (1861 – 1947) to create a logically unassailable foundation for mathematics, which culminated in their massive and ambitiously titled *Principia Mathematica***,** a work consisting of nearly 2000 pages which was published during the period 1910 – 1913 and whose title echoes Isaac Newton's monumental *Philosophiæ Naturalis Principia Mathematica*. The amount of detail in the work is illustrated by one frequently stated piece of trivia**;** namely**,** a proof that "$1 + 1 = 2$" does not appear until a few hundred pages into the book**.** The relevant page is depicted at following online site**:**

http://www.idt.mdh.se/~icc/1+1=2.htm

Some online references for the Russell – Whitehead *Principia* and a bibliographic reference are listed below. These include biographical references for the coauthors written from the perspective of philosophy as well as a biography of G. Frege (1848 – 1925), whose writings and ideas exerted a strong influence on the work of Russell and Whitehead.

B. Russell and A. N. Whitehead, ***Principia Mathematica*** (2nd Rev. Ed.), Cambridge University Press, Cambridge, UK, and New York, 1962. ISBN: 0–521–06791–X.

http://en.wikipedia.org/wiki/Alfred_North_Whitehead

http://plato.stanford.edu/entries/whitehead/

http://plato.stanford.edu/entries/russell/

http://plato.stanford.edu/entries/frege/

http://plato.stanford.edu/entries/principia-mathematica/

One disadvantage of the theory of types is the amount of duplication it requires; at each level one has an exact copy of the previous level. In some sense, von Neumann's Axiom of Foundation and the introduction of classes "too big" to be sets is a drastic simplification of the system of levels in the theory of types which still eliminates highly uncomfortable possibilities like $\mathbf{x} \in \mathbf{x}$.

IV : Relations and Functions

Mathematics and the other mathematical sciences are not merely concerned with listing objects. Analyzing comparisons and changes is also fundamentally important to the mathematical sciences and their applications. Binary and higher order relations are simple but important tools for studying mathematical comparisons, and in this unit we shall describe those aspects of binary relations that are particularly important in mathematics. Two particularly important types of relations are ***equivalence relations***, which suggest that related objects are interchangeable for certain purposes, and ***ordering relations***, which reflect the frequent need to say that one object in a set should come before another. Another important tool for studying comparison and change is the notion of a ***function***, which will also be covered in this unit.

IV .1 : Binary relations

(Halmos, § 6; Lipschutz, §§ 3.3 – 3.9, 3.11)

We shall only cover those aspects of the theory of binary relations that are needed to develop set theory. In particular, we shall not discuss the various algebraic operations and constructions on binary relations that exist and are useful in various practical contexts; these include the set – theoretic operations we have introduced more generally, but the algebra of binary relations has a considerable amount of additional structure. Much of this is summarized in the last two headings of Section 3.3 in Lipschutz and the subsequent material in Sections 3.4 – 3.7 of the same reference.

Many basic problems in computer science require extensive use of relations, and accordingly the latter are covered very extensively in discrete mathematics courses like Mathematics 11. Chapter 7 of Rosen contains a lengthy discussion of binary relations and **n** – ary relations for $\mathbf{n > 2}$, including numerous examples from computer science, the algebraic structure mentioned in the previous paragraph, various algebraic and graphical representations of relations, and some computational techniques and formulas.

The motivation for the mathematical study of relations is contained in the following quotation from page 471 of Rosen:

> *The most direct way to express a relationship between elements of two sets is to use ordered pairs made up of two related elements. For this reason, sets of ordered pairs are called binary relations.*

Formally, we proceed as follows:

Definition. If **A** and **B** are two classes, then a ***binary relation*** from **A** to **B** is a subset ***R*** of $\mathbf{A \times B}$. We shall often say that **x** *is* ***R*** *– related to* **y** or that **x** *is in the* ***R*** *– relation to* **y** if $\mathbf{(x, y) \in R}$. Frequently we shall also write **x** ***R*** **y** to indicate this relation holds for **x** and **y** in that order.

If $\mathbf{A = B}$, then a binary relation from **A** to **A** is simply called a ***binary relation on*** **A.**

Some binary relations are not particularly interesting. In particular, both the empty set and all of $\mathbf{A \times B}$ satisfy the condition to be a binary relation, but neither carries any information distinguishing one ordered pair **(a, b)** from another **(a′, b′).** A less trivial, but still relatively unenlightening, example of a binary operation on an arbitrary class **A** is given by the *diagonal relation* $\Delta_{\mathbf{A}}$ consisting of all pairs **(x, y)** such that $\mathbf{x = y}$. For the example $\boldsymbol{R = \Delta_A}$, the condition $\mathbf{x}\ \boldsymbol{R}\ \mathbf{y}$ simply means that **x** and **y** are equal.

In order to motivate the definition, we must construct further examples in which the given binary relation reflects something less trivial:

Technical comments on algebraic examples (may be skipped in the naïve approach). The examples below involve the standard number systems of mathematics and as such are basically algebraic in nature. Strictly speaking, it is necessary to introduce the relevant number systems formally in order to discuss such examples, but this poses no obstacles to an informal discussion and ultimately it is possible to justify everything in a logically rigorous manner; in particular, there are no surprises in doing so.

Algebraic Example IV.0.1. Let **A** be the integers, rational numbers or real numbers, and take the binary relation on **A** consisting of all **(x, y)** such that $\mathbf{x \leq y}$.

Algebraic Example IV.0.2. Let **A** be the integers, and take the binary relation on **A** consisting of all pairs **(x, y)** such that $\mathbf{x - y}$ is even. In this case **x** and **y** are related if and only if both are even or both are odd.

Algebraic Example IV.0.3. In this example **A** will correspond to the squares on a chessboard, so that

$$\mathbf{A = \{ 1, 2, 3, 4, 5, 6, 7, 8 \} \times \{ 1, 2, 3, 4, 5, 6, 7, 8 \}}$$

and **(x, y)** will be related to **(x′, y′)** if and only if one of the quantities $\mathbf{| x - x' |}$, $\mathbf{| y - y' |}$ is equal to 1 and the other is equal to 2. In nonmathematical terms this relation corresponds to the condition in chess that a knight positioned at square **(x, y)** is able to reach square **(x′, y′)** in one move provided the latter is not occupied by a piece of the same color.

Algebraic Example IV.0.4. In this example let **A** be the set of all polynomials with real coefficients, and stipulate that a polynomial **f(t)** is related to **g(t)** if there is a third polynomial **P(x)** such that $\mathbf{g(t) = P(f(t))}$.

A nonalgebraic example IV.0.5. This is given by the rock – paper – scissors game. Let **A** be the set **{ rock, scissors, paper },** and stipulate that object **x** is related to object **y** if object **x** wins over **y** under the usual rules of the game (**scissors** win over **paper,** while **paper** wins over **rock** and **rock** wins over **scissors**).

Abstract properties of binary relations

Certain important types of binary relations can be described by short lists of abstract properties. In this subsection we shall introduce these properties and determine whether they are true for various examples.

Definitions. Let ***R*** be a binary relation on a set **A.**

- ***R*** is said to be ***reflexive*** if $a \mathrel{R} a$ for all $a \in A$.
- ***R*** is said to be ***symmetric*** if $a \mathrel{R} b$ implies $b \mathrel{R} a$ for all $a, b \in A$.
- ***R*** is said to be ***transitive*** if $a \mathrel{R} b$ and $b \mathrel{R} c$ imply $a \mathrel{R} c$ for all $a, b, c \in A$.
- ***R*** is said to be ***antisymmetric*** if $a \mathrel{R} b$ and $b \mathrel{R} a$ imply $a = b$ for all $a, b \in A$.

The following result describes exactly which of these properties hold for each of the four examples described above.

Theorem 1. *The following are true for Algebraic Examples* **IV.0.1 – IV.0.4:**

The **first algebraic example** *is* **reflexive, antisymmetric** *and* **transitive** *but* **not symmetric.**

The **second algebraic example** *is* **reflexive, symmetric** *and* **transitive** *but* **not antisymmetric.**

The **third algebraic example** *is* **symmetric** *but* **not reflexive, antisymmetric** *or* **transitive.**

The **fourth algebraic example** *is* **reflexive** *and* **transitive** *but* **neither symmetric nor antisymmetric.**

Finally, the **nonalgebraic example** *is* **not symmetric, reflexive, antisymmetric** *or* **transitive.**

Proof. We begin with the first example. The first three of these are just basic properties of inequality. To see that such a relation is not symmetric it suffices to give an example of a pair **(x, y)** such that $x \leq y$ but the reverse inequality is false. The easiest way to give an example is to take $x = 0$ and $y = 1$.

Passing to the second example, it is reflexive because $x - x = 2 \cdot 0 = 0$. To see that it is reflexive, note that $x \mathrel{R} y$ implies $y - x = 2 \cdot n$ implies that $x - y = 2 \cdot (-n)$, which gives $y \mathrel{R} x$. Finally, if $x \mathrel{R} y$ and $y \mathrel{R} z$, then we have $y - x = 2 \cdot n$ and also $z - y = 2 \cdot m$, so that $z - x = 2 \cdot (m + n)$, which means that $x \mathrel{R} z$. Finally, to see that the relation is not antisymmetric, take $y = 2$ and $x = 0$. Then $x \mathrel{R} y$ and $y \mathrel{R} x$, but clearly **x** and **y** are not equal.

We now consider the third example. The relation is not symmetric because if we have $(x, y) \mathrel{R} (x', y')$ then both the first and second coordinates of **(x, y)** are unequal to the corresponding coordinates for **(x′, y′).** The defining condition for the relation remains the same if primed and unprimed variables are switched, and this means that the relation is symmetric. We now need to show that the relation is neither antisymmetric nor

transitive. To dispose of the first one, consider the ***R*** – related pairs $\mathbf{p = (1, 1)}$ and $\mathbf{q = (2, 3)}$. Then we have $\mathbf{p}\ \boldsymbol{R}\ \mathbf{q}$ and (since the relation is symmetric) $\mathbf{q}\ \boldsymbol{R}\ \mathbf{p}$, but clearly **p** and **q** are unequal. Finally, to show the relation is not transitive, let **p** and **q** be as in the previous sentences, and take $\mathbf{s = (3, 5)}$, so that $\mathbf{q}\ \boldsymbol{R}\ \mathbf{s}$. Then the absolute values of the differences of the coordinates for **p** and **s** are 2 and 4, so by the definition of ***R*** we cannot have $\mathbf{p}\ \boldsymbol{R}\ \mathbf{s}$. It might be helpful to get out a chessboard and experiment in order to obtain some additional insight into this example and the arguments given in this paragraph.

Next, we consider the fourth example. The relation is reflexive because if we take the identity polynomial $\mathbf{P(x) = x}$ then $\mathbf{f(t) = P(f(t))}$. Transitivity follows because if **Q** and **P** and polynomials then $\mathbf{Q[P(f(t))]}$ is again a polynomial in **f**. It remains to show the relation is neither symmetric nor antisymmetric. To see the relation is not symmetric take $\mathbf{f(t) = t}$ and $\mathbf{P(x) = x^2}$. Then we have $\mathbf{g(t) = t^2}$ and the lack of symmetry follows because the function **t** is not a polynomial in $\mathbf{t^2}$; a justification of this assertion is given in the footnote after the proof. To see that the relation is not antisymmetric, let us take $\mathbf{P(x) = x + 1}$ and $\mathbf{Q(x) = x - 1}$. Then for all **f** we have the identity

$$\mathbf{f(t) = Q[P(f(t))]} \quad \text{where} \quad \mathbf{P(f(t)) = f(t) + 1.}$$

Therefore we know that **f(t)** is ***R*** – related to $\mathbf{f(t) + 1}$ and vice versa. However, these two functions are never equal and therefore we have shown that $\mathbf{f}\ \boldsymbol{R}\ \mathbf{g}$ and $\mathbf{g}\ \boldsymbol{R}\ \mathbf{f}$ does not necessarily mean that $\mathbf{f = g}$. In other words, the relation is not antisymmetric.

Finally, we consider the nonalgebraic example. In this case the relation contains only three ordered pairs, and for each pair the coordinates are unequal. This shows the relation is not symmetric. It is also not transitive, for direct inspection shows that if $\mathbf{x}\ \boldsymbol{R}\ \mathbf{y}$ and $\mathbf{y}\ \boldsymbol{R}\ \mathbf{z}$ then we have $\mathbf{z}\ \boldsymbol{R}\ \mathbf{x}$ and we do not have $\mathbf{x}\ \boldsymbol{R}\ \mathbf{z}$. The validity of the symmetric property may seem surprising at first, but it turns out to be ***vacuously true*** because there are **NO** ordered pairs **(x, y)** such that $\mathbf{x}\ \boldsymbol{R}\ \mathbf{y}$ and $\mathbf{y}\ \boldsymbol{R}\ \mathbf{x}$.■

Footnote. In the course of the preceding argument, we asserted that the polynomial $\mathbf{g(t) = t}$ is not expressible as a polynomial in $\mathbf{f(t) = t^2}$. One way of proving this is to use the elementary identity

$$\textit{degree}\ \mathbf{[P(f(t))]} = \textit{degree}\ \mathbf{[f(t)]} \cdot \textit{degree}\ \mathbf{[P(x)]}.$$

If $\mathbf{g(t) = t}$ were expressible as a polynomial in $\mathbf{f(t) = t^2}$, then this would yield the equation $1 = 2 \cdot \textit{degree}\ \mathbf{[P(x)]}$, which is impossible because the degree of a nonzero polynomial is always a nonnegative integer.

As one might expect, it is also possible to construct other examples for which some properties hold and others do not. In particular, one can find examples that satisfy none of the four properties defined above.

Algebraic Example IV.0.5. Let **A** be the integers, rational numbers or real numbers, and take the binary relation on **A** consisting of all **(x, y)** such that $\mathbf{y = x + 1}$.

Discussion of this example. This relation is not reflexive because there are no numbers x such that $\mathbf{x = x + 1}$. It is not symmetric because $\mathbf{y = x + 1}$ implies $\mathbf{x = y - 1}$ and the right hand side of the second equation is not equal to $\mathbf{y + 1}$. It is also

not transitive, for $y = x + 1$ and $z = y + 1$ imply $z = x + 2$ and the right hand side of the last equation is not equal to $x + 1$. Finally, the relation is not antisymmetric, for there are no numbers x and y such that $y = x + 1$ and $x = y + 1$ (note that the two equations combine to imply $x = x + 2$ and $y = y + 2$).

Equivalence relations

Given a set **A,** one of the simplest but most important binary relations on **A** is given by equality; specifically, this is the relation E_A determined by the ***diagonal subset*** of $A \times A$ consisting of all ordered pairs **(a, b)** such that $a = b$.

Proposition 2. *For every set* **A** *the binary relation* E_A *is reflexive, symmetric and transitive.*

This result is merely a restatement of the three fundamental properties of equality; namely, **(1)** the reflexive property $x = x$, **(2)** the symmetric property $x = y \Rightarrow y = x$, and **(3)** the transitive property $x = y \ \& \ y = z \Rightarrow x = z$.■

Definition. A binary relation ***E*** on a set **A** is said to be an **equivalence relation** if it is reflexive, symmetric and transitive.

In addition to equality, our previous Algebraic Example **IV.0.2** is an equivalence relation. Yet another example may be obtained taking **A** to be the chessboard (or checkerboard?) set

$$A = \{ 1, 2, 3, 4, 5, 6, 7, 8 \} \times \{ 1, 2, 3, 4, 5, 6, 7, 8 \}$$

and choosing ***E*** such that **(x, y)** is ***E*** – related to **(x′, y′)** if and only if the sum

$$(x - x') + (y - y')$$

is even. In everyday terms, the condition on **(x, y)** and **(x′, y′)** means that the squares they represent have the same color. The verification that ***E*** is reflexive, symmetric and transitive is parallel to the corresponding argument for Algebraic Example **IV.0.2** above, and the details are left to the reader as an exercise.

One can also define an equivalence relation ***C*** on **A** by stipulating that **(x, y)** is ***C*** – related to **(x′, y′)** if and only if $y = y'$. It is immediate that **(x, y)** ***C*** **(x, y)** because $y = y$, while **(x, y)** ***C*** **(x′, y′)** implies $y = y'$, which further implies $y' = y$ so that **(x′, y′)** ***C*** **(x, y).** Finally, **(x, y)** ***C*** **(z, w)** and **(z, w)** ***C*** **(u, v)** imply $y = w$ and $w = v$, so that $y = v$ and therefore **(x, y)** ***C*** **(u, v).** Informally speaking, two elements of **A** are ***C*** – related if and only if the squares they represent are in the same column.

Definition. Let **A** be a set, and let ***E*** be an equivalence relation on **A.** For each $a \in A$, the ***E* – *equivalence class*** of **a,** written $[a]_E$ or simply **[a]** if ***E*** is clear from the context, is the set of all $x \in A$ such that x is ***E*** – related to a. — If **C** is an equivalence class for ***E*** and $x \in C$, then one frequently says that x *is a representative for the equivalence class* **C** (or something that is grammatically equivalent).

Since equivalence classes for ***E*** are subsets of **A,** we have the following elementary observation**.**

Proposition 3. *If* **A** *is a set and* ***E*** *is an equivalence relation on* **A,** *then the collection of all* ***E*** *– equivalence classes is a set.*

Proof. By construction the collection of all equivalence classes is a subcollection of the set **P(A).**■

As noted in Halmos**,** the set of all equivalence classes is often denoted by symbolism such as **A**/***E*,** and it is often verbalized as "**A** ***modulo*** ***E***" or (more briefly) "**A** ***mod*** ***E.***" Halmos also uses the notation **a**/***E*** for the equivalence class we (and most writers) denote by $[a]_E$**.**

Equivalence classes for previous examples. In Algebraic Example **IV.0.2,** the equivalence class of an integer **a** is the set of all even integers if a is even and the set of all odd integers if **a** is odd**.** For the equality relation(s)**,** the equivalence class of **a** is the set **{ a }** consisting only of **a.** In the first chessboard example**,** the equivalence class of a square is the set of all squares having the same color as the given one**,** and in the second example the equivalence class of a square is the set of all squares in the same column as the given one**.**

The equivalence classes of an equivalence relation have the following fundamentally important property:

Theorem 4. Let **A** be a set**,** suppose that **x** and **y** belong to **A,** and let ***E*** be an equivalence relation on **A.** Then either the equivalence classes $[x]_E$ and $[y]_E$ are disjoint or else they are equal**.**

Proof. Suppose that the equivalence classes in question are not disjoint**,** and let **z** belong to both of them**.** Then we have **x** ***E*** **z** and **y** ***E*** **z.** By symmetry**,** the second of these implies **z** ***E*** **y,** and one can combine the latter with **x** ***E*** **z** and transitivity to conclude that **x** ***E*** **y.**

Suppose now that $w \in [y]_E$**,** so that **y** ***E*** **w.** By transitivity and the final conclusion of the previous paragraph it follows that **x** ***E*** **w,** so that $w \in [x]_E$ is also true**.** Therefore we have shown that $[y]_E \subset [x]_E$**.** If we reverse the roles of **x** and y in this argument and note that **x** ***E*** **y** implies **y** ***E*** **x,** we can also conclude that $[y]_E \subset [x]_E$**.** Combining this with the preceding sentence yields the desired relationship $[y]_E = [x]_E$.■

Corollary 5. *The equivalence classes of an equivalence relation on* **A** *form a family of pairwise disjoint subsets whose union is all of* **A.**■

A converse to the preceding corollary also plays an important role in the study of equivalence relations**:**

Proposition 6. *Let* **A** *be a set, and let* **C** *be a family of subsets of* **A** *such that* **(1)** *the subsets in* **C** *are pairwise disjoint,* **(2)** *the union of the subsets is* **C** *is equal to* $\in$**.** *Then there is an equivalence relation* ***E*** *on* **A** *whose equivalence classes are the sets in the family* **C.**

The family **C** is said to define a ***partition*** of the set **A.**

Proof. We define a binary relation ***E*** on **A** by stipulating that **x *E* y** if and only if there is some **B** ∈ **C** such that **x** ∈ **B** and **y** ∈ **B.** Our first objective is to prove that ***E*** is an equivalence relation**.** To see that **x *E* x** for all **x,** let **x** be arbitrary and use the hypothesis that the union of the subsets in **C** is **A** to find some set **B** such that **x** ∈ **B.** We then have **x** ∈ **B** and **x** ∈ **B,** and therefore it follows that **x *E* x.** Now let **x *E* y;** then there is some **B** such that **x** ∈ **B** and **y** ∈ **B.** We then also have **x** ∈ **B** and **y** ∈ **B,** and therefore it follows that **y *E* x.** Finally**,** suppose that **x *E* y** and **y *E* z.** Then by the definition of ***E*** there are subsets **B, D** ∈ **C** such that **x** ∈ **B** and **y** ∈ **B** and also **y** ∈ **D** and **z** ∈ **D.** It follows that **B** and **D** have **y** in common**,** and since the family **C** of subsets is pairwise disjoint**,** it follows that the subsets **B** and **D** must be equal**.** But this means that **x** ∈ **B, y** ∈ **B** and **z** ∈ **B**. Therefore we have **y *E* z,** and this completes the proof that ***E*** is an equivalence relation**.**

What is the equivalence class of an element **x** ∈ **A?** Choose **B** such that **x** ∈ **B;** since **B** is the ***unique*** subset from the family **C** that contains **x,** it follows that **x *E* y** if and only if **y** also belongs to **B.** Therefore **B** is the equivalence class of **x.** Since **x** was arbitrary**,** this shows that the equivalence ***classes*** of ***E*** are just the subsets in the family **C.**■

Generating equivalence relations. Given a binary relation ***R*** on a set **A,** there are some situations where one wants to describe an equivalence relation ***E*** such that **x *E* y** if **x** and **y** are ***R*** – related**.** By the definition of a binary relation**,** this amounts to saying that ***R*** is contained in ***E*** as a subset of **A** × **A.** The following result shows that every binary relation ***R*** is contained in a *unique minimal* equivalence relation**:**

Theorem 7. *Let* **A** *be a set, and let* ***R*** *be a binary relation on* **A.** *Then there is a unique minimal equivalence relation* ***E*** *such that* ***R*** ⊂ ***E*.**

Proof. **(**)** Define a new binary relation ***E*** so that **x *E* y i**f and only if there is a finite sequence of elements of **A**

$$x = x_1, \ldots, x_n = y$$

such that for each **k** one (or more) of the following holds**:**

$$x_k = x_{k+1}$$

$$x_k \; R \; x_{k+1}$$

$$x_{k+1} \; R \; x_k$$

Suppose that ***F*** is an equivalence relation that contains ***R*** and that **x *E* y.** Then for each **k** it follows that $x_k \; F \; x_{k+1}$**,** and therefore by repeated application of transitivity it follows that **x *F* y.** Therefore**,** if ***E*** is an equivalence relation it will follow that it is the unique minimal equivalence relation containing ***R*.**

To prove that ***E*** is reflexive, for each **x** ∈ **A** it suffices to consider the simple length two sequence **x, x** and notice that the first option then guarantees that **x *E* x.** Suppose now that **x *E* y,** and take a sequence

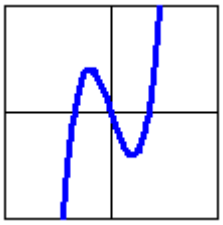
$$x = x_1, \ldots, x_n = y$$

as before. If we define a new sequence

$$y = y_1, \ldots, y_n = x$$

where $y_p = x_{n+1-p}$ then by the assumption on the original sequence we know that (at least) one of $y_p = y_{p+1}$, $y_{p+1}\ R\ y_p$, or $y_p\ R\ y_{p+1}$ holds. Therefore $y\ E\ x$, and hence the relation E is symmetric. Finally, suppose that $x\ E\ y$ and $y\ E\ z$. Then we have sequences $x = x_1, \ldots, x_n = y$ and $y = y_1, \ldots, y_m = z$ such that consecutive terms satisfy one of the three conditions listed above. Therefore if we define a new sequence whose terms w_p are given by x_p if $p \le n$ and by y_{p-n+1} if $p > n$, it will follow that consecutive terms satisfy one of the three conditions we have listed. This means that E is transitive and thus is an equivalence relation.■

Graphical example IV.0.7. Let X be the real numbers, and consider the binary relation $x\ R\ y$ if and only if $x^3 - 27x = y^3 - 27y$. It is fairly straightforward to verify that this defines an equivalence relation on the real numbers, and the equivalence classes consist of all values of x such that $x^3 - 27x$ is equal to a specific real number a. One way to visualize the equivalence classes of R is to take the graph of $x^3 - 27x$ and look at its intersection with a fixed horizontal line of the form $y = a$. If we sketch of the graph for $y = x^3 - 27x$ as in the picture below, it is apparent that for some choices of a one obtains equivalence classes with one point, for exactly two choices of a the equivalence classes consist of two points, and for still other choices the equivalence class consists of three points.



The cases with two points occur when the tangent line to the graph is horizontal, which happens when $|x| = 3$, and hence when $|a| = 54$. Thus equivalence classes have exactly one element if $|a| < 54$, exactly two elements if $|a| = 54$, exactly three elements if $|a| > 54$.

IV.2 : Partial and linear orderings

(Halmos, § 14; Lipschutz, §§ 3.10, 7.1 – 7.6)

In many areas of mathematics it is important to compare two objects of the same type and determine whether one is larger or smaller than the other. The real number system is one obvious example of this sort, but it is not the only one. When we consider the family of all subsets of a given set, it is often important to know if one subset is contained in another. In both cases the associated ordering by size can be expressed in terms of a binary relation, and these relations turn out to be reflexive, antisymmetric and transitive. These examples lead to a general concept.

Definition. If A is a set, then a ***partial ordering*** on **A** is a binary relation ***R*** on **A** which is reflexive, antisymmetric and transitive. A ***partially ordered set*** (or ***poset***) is an ordered pair **(A, *R*)** consisting of a set **A** together with a partial ordering ***R*** on **A.**

If the partial ordering ***R*** is clear or unambiguous from the context, we often write $x \; R \; y$ in a more familiar form like $x \leq y$ or $y \geq x$. Similarly, if $x \leq y$ but $x \neq y$ then we often write $x < y$ or $y < x$ and say either that **x** *is strictly less than* **y** or equivalently that **y** *is strictly greater than* **x.**

Standard example IV.0.8. The real number system $\mathbb{R}$ with the usual meaning of "**<**" as "***is less than***" clearly satisfies the conditions for a partial ordering.

Set – theoretic example IV.0.9. If **S** is a set, then the set – theoretic inclusion relation $A \subset B$ on the power set **P(S)** is a partial ordering by the results of Unit **II.**

These are the most basic examples of partial orderings, but there are also many others that arise naturally.

Algebraic Example IV.0.10. Let **A** be the positive integers and let ***R*** be the binary relation $x \; R \; y$ if and only if **y** is evenly divisible by **x** (with no remainder, so that $y = xz$ for some positive integer **z**). The relation is reflexive because $x = x \cdot 1$. To see that the relation is antisymmetric, suppose that $y = xz$ and $x = yw$. Combining these, we obtain the equation $x = xzw$, where **x, z** and **w** are all positive integers. The only way one can have an equation of this sort over the positive integers is if $z = w = 1$. To see that the relation is transitive, suppose that $y = xu$ and $z = yv$. Combining these, we see that $z = yvu$, where **y, v** and **u** are all positive integers. This implies that $x \; R \; z$.

Algebraic Example IV.0.11. Once again, take **A** to be the chessboard (or should it be checkerboard?) set

$$A = \{ 1, 2, 3, 4, 5, 6, 7, 8 \} \times \{ 1, 2, 3, 4, 5, 6, 7, 8 \}$$

and start with the standard ordering on the first eight positive integers. One then has the so – called ***lexicographic*** or ***dictionary ordering*** on **A** such that $(x, y) \leq (x', y')$ if and only if either **(1)** $x < x'$ or else **(2)** $x = x'$ and $y \leq y'$. We shall show this is a partial ordering by proving a more general statement.

Proposition 1. *Suppose that* **P** *and* **Q** *are partially ordered sets (with orderings denoted by* $\leq_P$ *and* $\leq_Q$*), and define a binary relation* $\leq$ *(the* ***lexicographic*** *or* ***dictionary*** *ordering) on the product* $P \times Q$ *by* $(x, y) \leq (x', y')$ *if and only if either* **(1)** $x <_P x'$ *or else* **(2)** $x = x'$ *and* $y \leq_Q y'$. *Then the relation* $\leq$ *defines a partial ordering on* $P \times Q$.

Before beginning the proof, note that in all cases $(x, y) \leq (x', y')$ implies $x \leq_P x'$.

Proof. We being by showing it is reflexive. By Condition **(2)** we have $(x, y) \leq (x, y)$. Suppose now that we have both $(x, y) \leq (x', y')$ and $(x', y') \leq (x, y)$. Then **(1)** and **(2)** combine to show that $x \leq_P x'$ and $x' \leq_P x$; therefore we must have $x = x'$. We can now apply **(2)** to conclude that $y \leq_Q y'$ and $y' \leq_Q y$, and hence that $y = y'$. Thus both coordinates of (x, y) and (x', y') are equal, and consequently the two ordered pairs are equal. Finally, suppose that we have $(x, y) \leq (z, w)$ and also $(z, w) \leq (u, v)$. The remaining argument splits into cases; as noted before, by definition of the relation, if two ordered pairs **(a, b)** and **(c, d)** are related then $a \leq c$. ***Case 1:*** Suppose we have either

$x <_P z$ or $z <_P u$. In either case we have $x < u$ and therefore by Condition **(1)** we have $(x, y) \leq (u, v)$. ***Case 2*:** Suppose that $x = z = u$. In this case Condition **(2)** implies $y \leq_Q w$ and $w \leq_Q v$, and by transitivity of $\leq$ it follows that $y \leq_Q v$. Combining the statements in the last two sentences, we conclude that $(x, y) \leq (u, v)$. This completes the proof of transitivity. ■

Linear orderings

One major difference between the ordering of the real numbers and the ordering of a set of subsets is that real numbers satisfy the following ***trichotomy principle:***

For every **x** *and* **y**, **exactly one** *of* $x = y$, $x < y$ *or* $y < x$ *is true*.

It is easy to construct examples showing this fails for a set of subsets **P(A)**. Specifically, if $A = \{1, 2\}$ with $x = \{1\}$ and $y = \{2\}$, then **x** and **y** are distinct but neither is a subset of the other.

We can formalize this property of real numbers by means of another definition.

Definition. Let **(A, *R*)** be a partially ordered set. Then ***R*** is said to be a ***linear ordering***, a ***simple ordering*** or a ***total ordering*** if for every pair of elements **x** and **y** in **A**, we either have **x *R* y** or **y *R* x**. — Since a partial ordering is antisymmetric, both conditions hold if and only if $x = y$.

Here are two simple but useful results on partially ordered sets.

Proposition 2. *Let* **(A, *R*)** *be a partially ordered set, let* **B** *be a subset of* **A**, *and let* ***R*|B** *be the restricted binary relation on* **B** *defined by* $R \cap (B \times B)$. *Then* ***R*|B** *is a partial ordering on* **B**. *Furthermore, if* ***R*** *is a linear ordering then so is* ***R*|B**.

The key observation in the proof is that if **x** and **y** belong to **B**, then **x *R*|B y** if and only if **x *R* y**. Details of the argument are left to the reader as an exercise. ■

Proposition 3. *Let* **(A, *R*)** *be a partially ordered set, and let* R^{OP} *denote the converse relation* **x** R^{OP} **y** *if and only if* **y *R* x**. *Then* R^{OP} *defines a partial ordering on* **A**. *Also, if* ***R*** *is a linear ordering then so is* R^{OP}.

The relation R^{OP} defines the ***opposite*** or ***reverse partial ordering*** of ***R*** in which the roles of "$\leq$" and "$\geq$" are switched. The verification of this result is also fairly elementary and left to the reader as an exercise. ■

Proposition 4. ("Dictionary Theorem") *If* **A** *and* **B** *are linearly ordered sets, then the product* $A \times B$ *with the lexicographic ordering is also linearly ordered.*

Proof. Suppose we are given **(a, b)** and **(a′, b′)**. Since **A** is linearly ordered, exactly one of the statements $a <_A a'$, $a = a'$ or $a >_A a'$ is true. In the first and third cases we have $(a, b) < (a', b')$ and $(a, b) > (a', b')$ respectively.

Suppose now that **a = a′;** since **B** is linearly ordered, exactly one of $\mathbf{b <_B b'}$, **b = b′** or $\mathbf{b >_B b'}$ is true. In the respective cases we have **(a, b) < (a′, b′), (a, b) = (a′, b′)** and **(a, b) > (a′, b′).**■

Partially ordered sets arise in many different mathematical contexts**,** and this wide range of contexts generates a long list of properties that a partially ordered set may or may not satisfy**.** Several of these are described on pages 54 – 58 of Halmos**.** We shall discuss a few of these together with some examples for which the properties are true and others for which the properties are false**.**

Definitions. An element **x** in a partially ordered set **A** has an ***immediate predecessor*** if there is a maximal **y** such that **y < x.** An element **x** in a partially ordered set **A** has an ***immediate successor*** if there is a minimal **y** such that **y > x.**

The integers have the property that every element has an immediate predecessor and an immediate successor**,** while the real numbers have the property that no element has an immediate predecessor of an immediate successor**.** If we remove the subset of all real numbers **x** such that **0 < |x| < 1** and **1 < |x| < 2,** then some elements will have immediate predecessors**,** some will have immediate successors**,** some will have both**,** and others will have neither**.**

Definition. A partially ordered set **A** is ***finitely bounded from above*** if for every pair of elements **x** and **y** in **A** there is some **z ∈ A** such that **x, y ≤ z.** Similarly**,** a partially ordered set **A** is ***finitely bounded from below*** if for every pair of elements **x** and **y** there is some **z ∈ A** such that **z ≤ x, y.**

Every linearly ordered set is finitely bounded from above and below (take the larger or smaller of the two elements)**.** Furthermore**,** every power set **P(A)** is also finitely bounded from above and below (given **x** and **y,** their union contains both and their intersection is contained in both). If **A** is a set with more than one element, then the set **X ⊂ P(A)** of all subsets with exactly one element is neither finitely bounded from above nor finitely bounded from below**.**

Definition. A partially ordered set **A** is a ***lattice*** if the following conditions hold**:**

(a) For all **x, y ∈ A** there is a ***unique minimal*** **z ∈ A** such that **x, y ≤ z.**

(b) For all **x, y ∈ A** there is a ***unique maximal*** **z ∈ A** such that **z ≤ x, y.**

Examples of lattices. 1. Every linearly ordered set is a lattice, for if **x ≤ y** then **y** is the unique minimal **z** such that **x, y ≤ z** and **x** is the unique maximal **z** such that **z ≤ x, y;** similarly, if **y ≤ x** then **x** is the unique minimal **z** such that **x, y ≤ z** and **y** is the unique maximal **z** such that **z ≤ x, y.**

2. Every power set **P(A)** is a lattice (with inclusion as the partial ordering)**.** Given two subsets **B, C ⊂ A,** the union **B ∪ C** is the unique minimal **Z** such that **B, C ⊂ Z** and the intersection **B ∩ C** is the unique maximal **Z** such that **Z ⊂ B, C.**

3. Let $\mathbf{VecSub}(\mathbb{R}^n)$ denote the set of vector subspaces of $\mathbb{R}^n$ with inclusion as the partial ordering**.** Given two vector subspaces **X, Y** of $\mathbb{R}^n$ the linear sum **X + Y** is the unique minimal **Z** such that **X, Y ⊂ Z** and the intersection **X ∩ Y** is the unique maximal

Z such that $\mathbf{Z} \subset \mathbf{X}, \mathbf{Y}$. Note that the ordering in this example is the restriction of the ordering in the previous one but the unique minimal **Z** changes. This reflects the fact that $\mathbf{X} + \mathbf{Y}$ is the unique smallest subspace which contains the subset $\mathbf{X} \cup \mathbf{Y}$.

On the other hand, if **X** is a reasonably large finite set then the set $\mathbf{C} \subset \mathbf{P(X)}$ of all subsets ***not containing exactly two specific elements*** of **X** is finitely bounded from above and below, but ***it is not a lattice*** (given two distinct one point subsets, there are several subsets containing both of them, but there is no unique minimal set of this type).

The following type of partially (in fact, linearly) ordered set plays an important role in the mathematical sciences.

Definition. A partially ordered set **A** is said to be ***well – ordered*** if every nonempty subset has a minimal element.

Algebraic Example IV.0.12. If **A** denotes the nonnegative integers and one takes the usual ordering, then **A** is well – ordered; we shall say more about this in the next unit. — One can also construct other well – ordered sets. For example, if **A** denotes the nonnegative integers and $\mathbf{B} \notin \mathbf{A}$, consider the partial ordering on $\mathbf{A} \cup \{\mathbf{B}\}$ which restricts to the usual ordering on **A** and has **B** as a unique maximal element. Similarly, if we take some **C** such that $\mathbf{C} \notin \mathbf{A} \cup \{\mathbf{B}\}$, then we can construct an extended well – ordering on the set $\mathbf{A} \cup \{\mathbf{B}, \mathbf{C}\}$ for which **C** is the unique maximal element. Constructions of this sort played a significant role in Cantor's work on trigonometric series which led him to develop set theory.

Proposition 5. *Every well – ordered set is linearly ordered.*

Proof. Let **A** be the well – ordered set. If **A** does not have at least two elements then there is nothing to prove, so assume that **A** does have at least two elements. Suppose that **x** and **y** are distinct elements of **A**, and consider the nonempty subset $\{\mathbf{x}, \mathbf{y}\}$. By the well – ordering assumption we know this set has a least element. If it is **x**, then we have $\mathbf{x} < \mathbf{y}$, and if it is y then we have $\mathbf{y} < \mathbf{x}$. ■

Product orderings

Definition. Let **A** and **B** be partially ordered sets. Define a binary relation ***P*** on the product $\mathbf{A} \times \mathbf{B}$ by $(\mathbf{a}, \mathbf{b})\ \boldsymbol{P}\ (\mathbf{a}', \mathbf{b}')$ if and only if $\mathbf{a} \leq \mathbf{a}'$ and $\mathbf{b} \leq \mathbf{b}'$. The relation ***P*** is called the *product partial ordering* on $\mathbf{A} \times \mathbf{B}$, and this usage is justified by the following result:

Theorem 6. *If* **A** *and* **B** *are partially ordered sets as above, then* ***P*** *is a partial ordering on* $\mathbf{A} \times \mathbf{B}$.

Proof. The reflexive property $(\mathbf{a}, \mathbf{b})\ \boldsymbol{P}\ (\mathbf{a}, \mathbf{b})$ follows from $\mathbf{a} \leq \mathbf{a}$ and $\mathbf{b} \leq \mathbf{b}$. To see that ***P*** is symmetric, suppose that $(\mathbf{a}, \mathbf{b})\ \boldsymbol{P}\ (\mathbf{a}', \mathbf{b}')$ and $(\mathbf{a}', \mathbf{b}')\ \boldsymbol{P}\ (\mathbf{a}, \mathbf{b})$. Then we have $\mathbf{a} \leq \mathbf{a}'$ and $\mathbf{a}' \leq \mathbf{a}$, so that $\mathbf{a} = \mathbf{a}'$. Similarly, we have have $\mathbf{a} \leq \mathbf{a}'$ and $\mathbf{a}' \leq \mathbf{a}$, so that $\mathbf{a} = \mathbf{a}'$; combining these, we conclude that $(\mathbf{a}, \mathbf{b}) = (\mathbf{a}', \mathbf{b}')$. To show ***P*** is transitive, suppose that $(\mathbf{a}, \mathbf{b})\ \boldsymbol{P}\ (\mathbf{a}', \mathbf{b}')$ and $(\mathbf{a}', \mathbf{b}')\ \boldsymbol{P}\ (\mathbf{a}'', \mathbf{b}'')$. Then $\mathbf{a} \leq \mathbf{a}'$ and $\mathbf{a}' \leq \mathbf{a}''$ imply $\mathbf{a} \leq \mathbf{a}''$, and similarly $\mathbf{b} \leq \mathbf{b}'$ and $\mathbf{b}' \leq \mathbf{b}''$ imply $\mathbf{b} \leq \mathbf{b}''$. Combining these, we have $(\mathbf{a}, \mathbf{b})\ \boldsymbol{P}\ (\mathbf{a}'', \mathbf{b}'')$. This completes the proof

that ***P*** defines a partial ordering on $\mathbf{A \times B}$.■

It is natural to ask how the product ordering ***P*** is related to the lexicographic ordering ***L*** constructed above. Here is a partial answer.

Theorem 7. *If* ***L*** *and* ***P*** *respectively denote the lexicographic and partial orderings on* $\mathbf{A \times B}$, *then* $\mathbf{(a, b)\ P\ (a', b')}$ *implies* $\mathbf{(a, b)\ L\ (a', b')}$.

In a situation like this one often says that the partial ordering ***L*** is a ***refinement*** of the partial ordering ***P***.

Proof. If $\mathbf{(a, b)\ P\ (a', b')}$, then $\mathbf{a \le a'}$. If $\mathbf{a < a'}$, then by definition we have $\mathbf{(a, b)\ L\ (a', b')}$. On the other hand, if $\mathbf{a = a'}$, then since $\mathbf{b \le b'}$ we also have $\mathbf{(a, b)\ L\ (a', b')}$ in this case.■

Example. Usually the lexicographic ordering is a **strict** refinement of the product ordering; ***i.e.***, there are pairs **(a, b)** and **(c, d)** such that $\mathbf{(a, b)\ L\ (c, d)}$ is true but $\mathbf{(a, b)\ P\ (c, d)}$ is false. Consider the linearly ordered set consisting of the ordinary alphabet

$$\mathbf{A = \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z\}}$$

with the usual alphabetical ordering. Then **(a, z)** precedes **(b, a)** in the lexicographic ordering but not in the product ordering. Of course, **(b, a)** does not precede **(a, z)** in either ordering.

Further topics. Sections 7.3, 7.4 and 7.10 – 7.11 in Lipschutz contain additional material on partial orderings which goes beyond these notes. Toplcs include additional methods for constructing new partial ordering out of old ones, graphical representations of partial orderings, additional terminology, and more detailed discussions of a few special types of partially ordered sets (for example, lattices). Some of this material is used in a few of the exercises.

IV.3: Functions

(Halmos, §§ 8 – 10; Lipschutz, §§ 4.1 – 4.4, 5.6, 5.8)

When one thing depends on another, as, for example, the area of a circle depends on the radius, or the temperature on the mountain depends on the height, or the underwater pressure depends upon the depth, then we say that the first is a "**function**" of the other.

More generally, if the value of a quantity **y** belongs to **B** and depends upon the value of a quantity **x** which belongs to **A,** we can say that the value of **y** in **B** is a ***function*** of the value of **x** in **A.** Taking this one step further, we can say that the function **f** is a rule which associates to each element $\mathbf{a \in A}$ some unique element $\mathbf{b \in B}$, and this is frequently written symbolically as $\mathbf{b = f(a)}$.

The concept of a function is absolutely central to the mathematical sciences and to every specialized branch of mathematics. For example, the following two reasons for the importance of functions reflect comments at the beginning of the previous section:

1. Functions can be used to describe how a given object is related to another one.
2. Functions serve particularly well as abstract mathematical models for changes in the real world.

In light of the second point, it should not be surprising that mathematicians often use dynamic words like ***mapping***, ***morphism*** or ***transformation*** as synonyms for function.

In fact, it is even possible to develop the foundations of mathematics in a logically rigorous manner using functions as the primitive notion rather than sets, but we shall not attempt to discuss this alternative approach here (in particular, it requires a higher degree of abstraction than is otherwise necessary). However, here are some references for this approach and its background:

http://en.wikipedia.org/wiki/Category_theory

http://plato.stanford.edu/entries/category-theory/

www.cs.toronto.edu/~sme/presentations/cat101.pdf

http://www.pnas.org/cgi/reprint/52/6/1506.pdf

Standard methods of describing functions

Basic mathematics courses in calculus and other subjects give several ways of describing functions. Here are a few standard examples:

1. The use of ***tables*** to ***list the values*** of functions in terms of their dependent variables.
2. The use of ***formulas*** to ***express the values*** of functions in terms of their dependent variables.
3. The use of ***graphs*** to ***visualize the behavior*** of functions.

Each of these methods is quite old. A complete discussion of the historical background is beyond the scope of these notes, but a few remarks seem worthwhile.

Tables of values. Although our knowledge of mathematics in the earliest civilizations is limited, we do have examples of tables in both Egyptian and Babylonian mathematics from well before 1500 B. C. E., and extensive, fairly accurate tables of trigonometric functions had been compiled between 1000 and 2000 years ago in several ancient civilizations.

Formulas. The concept of a formula was at least informally understood in ancient civilizations in numerous locations throughout the world, and verbally stated functions are certainly explicit in classical Greek and Indian mathematics. In particular, there are many verbal (also called *rhetorical*) formulas in Euclid's ***Elements***. Of course, symbolic expressions of formulas require some form of mathematical symbolism. The development of the latter took place in an uneven manner over several centuries; in Western civilization, Diophantus of Alexandria introduced systematic notational abbreviations for basic mathematical concepts during the 3rd century A. D. Eventually such abbreviations and symbolisms were employed to express mathematical formulas,

but this really did not become very well established in Western mathematics until later in the 16th century, particularly in the work of R. Bombelli (1526 – 1572) and F. Viète (1540 – 1603).

Graphs. The idea of representing a function graphically dates back (at least) to N. Oresme (1323 – 1382; pronounced o-**REMM**), and it is described in the book, *Tractatus de figuratione potentiarum et mensurarum* ("Latitude of Forms"), which was written either by him or one of his students; this book was extremely influential over the next three centuries, and in particular the impact can be seen in the scientific work of Galileo (G. Galilei, 1564 – 1642). In fact, the graphical representation of a function provides one motivation for the standard mathematical definition of a function.

The formal definition of a function

The use of the word "function" to denote the relationship between a dependent and independent variable is due to G. W. von Leibniz (1646 – 1716), who introduced the term near the end of the 17th century. Over the next 150 years there was a great deal of discussion about exactly how a function should be defined, and during that time the standard **f(x)** notation, in which the latter expression represents the dependent variable and **x** represents the independent variable, was introduced by L. Euler (1706 – 1783). In the first half of the 19th century P. Lejeune – Dirichlet (1805 – 1859; the last part of the name is pronounced də-**REESH**-lay) and N. Lobachevsky (1792 – 1856) independently and almost simultaneously gave the modern definition of function as a fairly arbitrary rule assigning a unique value to each choice for the independent variable. A brief but very informative summary of the evolution of the concept of a function appears on pages 73 – 75 of the following textbook:

> Z. Usiskin, A. Peressini, E. A. Marchisotto, and D. Stanley, ***Mathematics for High School Teachers: An Advanced Perspective.*** *Prentice – Hall,* Upper Saddle River, NJ, 2002. ISBN: 0–130–44941–5.

Formally this association can be done in several ways, but the most common is by means of ordered pairs, and we shall also employ this approach. It follows that, from a purely formal viewpoint,

a function is essentially a special type of binary relation.

Definition. A ***function*** is an ordered pair $(\mathbf{A}, \mathbf{B}), \Gamma)$ where **A** and **B** are sets and Γ is a subset of $\mathbf{A} \times \mathbf{B}$ with the following property:

[! !] *For each* $\mathbf{a} \in \mathbf{A}$ *there is a* **unique** *element* $\mathbf{b} \in \mathbf{B}$ *such that* $(\mathbf{a}, \mathbf{b}) \in \Gamma$.

The sets **A** and **B** are respectively called the ***domain*** and ***codomain*** of **f**, and Γ is called the ***graph*** of **f**. Frequently we write $\mathbf{f} : \mathbf{A} \to \mathbf{B}$ to denote a function with domain **A** and codomain **B**, and as usual we write

$\mathbf{b} = \mathbf{f(a)}$ *if and only if the ordered pair* $(\mathbf{a}, \mathbf{b})$ *lies in the graph of* **f**.

By **[! !]**, for every $\mathbf{a} \in \mathbf{A}$ there is a unique $\mathbf{b} \in \mathbf{B}$ such that $\mathbf{b} = \mathbf{f(a)}$.

Frequently a function is simply defined to be the subset Γ described above, but in our definition the source set **A** (formally, this is the ***domain*** of the function) and the target set **B** (formally, this is the ***codomain*** of the function) are included explicitly as part of the structure. The domain is essentially redundant; however, in some mathematical contexts if $f : A \to B$ is a function and **B** is a subset of **C,** then from our perspective it is *absolutely necessary* to distinguish between the function from **A** to **B** with graph Γ and the analogous function from **A** to **C** whose graph is also equal to Γ. One can also take this in the reverse direction; if $f : A \to B$ is a function such that its graph Γ lies in $A \times D$ for some subset $D \subset B$, then it is often either convenient or even mandatory to view the graph as also defining a related function $f : A \to D$.

The need to specify codomains is fundamentally important in computer science; for example, in computer programs one must often declare whether the values of certain functions should be integer variables or real (floating point) variables. A basic mathematical example at a more advanced level is discussed in Chapter 9 of the previously mentioned book by Munkres.

Variants of the main definition. We have defined functions to be *total* (*i.e.*, it has a value for every argument in the domain), following usual mathematical practice. A *partial function* is a function which need not be defined on every member of its domain; however, one still insists that for each $x \in A$ there is at most one $y \in B$ such that a pair of the form **(x, y)** lies in the graph. Some references go even further and talk about *multiple valued functions* such that for a given **x** there may be more than one **y** such that **(x, y)** lies in the graph. However, such objects will not be discussed any further in these notes. All functions considered here will be ***single valued.***

Example. If **A** is the set of real numbers, then the function **f(x)** given by the standard formula x^2 is given formally by **(**(**A, A**), **G)** where **G** denotes the set of all **(x, y)** in the product $A \times A$ such that $y = x^2$. Similar considerations apply for most of the functions that arise in differential and integral calculus.

One disadvantage of our definition is that it does not allow us to define functions whose domains or codomains are classes but not necessarily sets. Such objects are needed at certain points in Unit V and in order to accommodate them we shall make the following nonstandard definition.

Definition. If **A** and **B** are classes, then a *graph* (or *prefunction*) on $A \times B$ will be a subset of $A \times B$ satisfying **[! !]**.

Example(s). A simple example of a prefunction on the universal class U^* of all sets is given by the set of all ordered pairs $(S, P(S))$ where **S** is an arbitrary set.

Here is another nontrivial example of a prefunction on the universal class U^* of all sets; it is related to some constructions in Section V.3: Take Σ to be the collection of all ordered pairs **(x, y)** such that **x** is a set and $y = x \cup \{x\}$ (strictly speaking the definition of this class requires a slightly stronger version of the Axiom of Specification than we have used, so that one can define classes that are not necessarily contained in

some fixed set; for example, one can use Axiom ***ZF4*** on page 82 of the book by Goldrei that was cited at the beginning of these notes).

Equality of functions

In both the naïve and formal approaches to set theory, one of the first things is to state the standard criterion for two sets to be equal. We shall begin the discussion of this section by verifying the standard fundamental criterion for two functions to be equal.

Proposition 1. Let $f : A \to B$ *and* $g : A \to B$ *be functions. Then* $f = g$ *if and only if* $f(x) = g(x)$ *for every* $x \in A$.

Proof. If $f = g$ then their graphs are equal to the same set, which we shall call G. By definition of a function, for each $x \in A$ there is a unique $b \in B$ such that $(x, b) \in G$, and it follows that b must be equal to both $f(x)$ and $g(x)$. Conversely, if $f(x) = g(x)$ for every $x \in A$, then for each we know that the graphs of f and g both contain the element (x, b) where $b = f(x) = g(x)$. Since for each x the graphs of f and g each contain exactly one point whose first coordinate is x, it follows that these graphs are equal. By the definition of a function, this implies $f = g$.■

Images and inverse images

Definition. Let $f : A \to B$ be a function, and let $C \subset A$. Then *the image of* C *under* (*the mapping*) f is the set

$$f[C] = \{ y \in B \mid y = f(x) \text{ for some } x \in A \}.$$

Similarly, if $D \subset B$, then *the inverse image of* D *under* (*the mapping*) f is the set

$$f^{-1}[D] = \{ x \in A \mid f(x) \in D \}.$$

The set $f[A]$, which is the image of the entire domain under f, is often called the ***range*** of the function.

Comment on notation. One often uses parentheses rather than brackets and writes images and inverse images as $f(C)$ and $f^{-1}(D)$ rather than $f[C]$ and $f^{-1}[D]$. In most cases this should cause no confusion, but there are some exceptional situations where problems can arise, most notably if the set $Y = A$ or B contains an element x such that both $x \in A$ and $x \subset A$. Such sets are easy to manufacture; in particular, given a set x we can always form $A = x \cup \{ x \}$, but in practice the replacement of brackets by parentheses is almost never a source of confusion. We shall consistently use square brackets to indicate images and inverse images.

By definition we know that $\{ f(x) \} = f[\{ x \}]$. One often also sees ***abuses of notation*** in which an inverse image of a one point set $f^{-1}[\{ y \}]$ is simply written in the abbreviated form $f^{-1}(y)$. In such cases it is important to recognize that the latter is a ***subset*** of the domain and ***not an element*** of the latter (in particular, the subset may be empty or contain more than one element).

Examples. **1.** Suppose that **A = B** is the real number system, $\mathbf{f(x) = x^2}$ and **C** is the closed interval **[2, 3].** Then **f[C]** is equal to the closed interval **[4, 9],** and if **C** is the closed interval **[– 1, 1]** then **f[C]** is equal to the closed interval **[0, 1].** Similarly, if **D** is the closed interval **[16, 25]** then $\mathbf{f^{-1}[D]}$ equals the union of the two intervals **[– 5, – 4]** and **[4, 5],** while if **D** is the closed interval **[– 9, 4]** then $\mathbf{f^{-1}[D]}$ equals the closed interval **[– 2, 2].**

2. Let **f(x) = 2x,** and let **E** be the interval **[a, b].** Then the image **f[E] = [2a, 2b]** and the inverse image $\mathbf{f^{-1}[E] = [½a, ½b].}$ Note that the range of **f,** which is the image of the entire domain, is just the set of all real numbers.

3. Let $\mathbf{f(x) = x^2.}$ If **E = [–1, 2],** then **f[E] = [0, 4].** Similarly, if either **E = [–1, 4]** or **E = [–2, 4],** then $\mathbf{f^{-1}[E] = [0, 2].}$ The two sets have the same inverse image because there is no real number **x** whose square is negative**.** Note that the range of **f,** which is the image of the entire domain**,** is just the set of all nonnegative real numbers**.**

In order to work a change of variables problem in multivariable calculus it is usually necessary to find the image or the inverse image of a set under some vector valued function of several variables**.** Examples and exercises of this sort are given in Section 6.1 of the previously cited book by Marsden and Tromba**.**

The following basic identities involving images and inverse images are mentioned (and in a few cases verified) on pages 38 – 39 of Halmos**.**

Theorem 2. *If* $\mathbf{f : A \to B}$ *is a function, then the image and inverse image constructions for* **f** *have the following properties:*

1. *If* **V** *is a family of subsets of* **A,** *then* $\mathbf{f[\cup_{C \in V} C] = \cup_{C \in V} f[C].}$
2. *If* **V** *is a nonempty family of subsets of* **A,** *then we have* $\mathbf{f[\cap_{C \in V} C] \subset \cap_{C \in V} f[C]}$ *and the containment is proper in some cases.*
3. *If* **C** *is a subset of* **A,** *then* $\mathbf{C \subset f^{-1}[f[C]].}$
4. *If* **W** *is a family of subsets of* **B,** *then we have* $\mathbf{f^{-1}[\cup_{D \in W} D] = \cup_{D \in W} f^{-1}[D].}$
5. *If* **W** *is a nonempty family of subsets of* **B,** *then we have* $\mathbf{f^{-1}[\cap_{D \in W} D] = \cap_{D \in W} f^{-1}[D].}$
6. *If* **D** *is a subset of* **B,** *then* $\mathbf{f[f^{-1}[D]] \subset D.}$
7. *If* **D** *is a subset of* **B,** *then* $\mathbf{f^{-1}[B - D] = A - f^{-1}[D].}$

Proof. Each statement requires separate consideration.

Verification of **(1):** Suppose that $\mathbf{y \in f[\cup_{C \in V} C].}$ Then **y = f(x)** for some element **x** belonging to $\mathbf{\cup_{C \in V} C,}$ and for the sake of definiteness let us say that $\mathbf{x \in C_0.}$ It follows that $\mathbf{y \in f[C_0],}$ and since the latter is contained in $\mathbf{\cup_{C \in V} f[C]}$ it follows that

the original element **y** belongs to $\cup_{C \in V} f[C]$. Conversely, if $y \in \cup_{C \in V} f[C]$ and we choose C_0 so that $y \in f[C_0]$, then $y = f(x)$ for $x \in C_0$ and $C_0 \subset \cup_{C \in V} C$ combine to imply that $y \in f[\cup_{C \in V} C]$. Hence the two sets in the statement are equal.

Verification of **(2):** Suppose that $y \in f[\cap_{C \in V} C]$. Then $y = f(x)$ for some element **x** belonging to $\cap_{C \in V} C$, and therefore $y \in f[C]$ for each $C \in V$. But this means that **y** belongs to $\cap_{C \in V} f[C]$, and this proves the containment assertion. To see that this containment may be proper, consider the function x^2 from the real numbers to themselves, and let **B** and **C** denote the closed intervals $[-1, 0]$ and $[0, 1]$ respectively. Then $f[B \cap C] = \{0\}$ but $f[B] \cap f[C] = [0, 1]$.

Verification of **(3):** If $x \in C$ then $f(x) \in f[C]$, and therefore $x \in f^{-1}[f[C]]$, proving the containment assertion.

Verification of **(4):** Suppose that $x \in f^{-1}[\cup_{D \in W} D]$. By definition we then know that $f(x) \in \cup_{D \in W} D$, and for the sake of definiteness let us say that $f(x) \in D_0$. Then we have $x \in f^{-1}[D_0]$, and since the latter is contained in $f^{-1}[\cup_{D \in W} D]$ we conclude that $f^{-1}[\cup_{D \in W} D] = \cup_{D \in W} f^{-1}[D]$. Conversely, let $x \in \cup_{D \in W} f^{-1}[D]$. Once again, for the sake of definiteness choose D_0 so that $x \in f^{-1}[D_0]$. We then have that $f(x) \in D_0$, where the latter is contained in $\cup_{D \in W} D$, so that $f(x)$ must belong to the set $\cup_{D \in W} D$. This implies that $x \in f^{-1}[\cup_{D \in W} D]$. Therefore we have shown that each of the sets under consideration is contained in the other and hence they must be equal.

Verification of **(5):** Suppose that $x \in f^{-1}[\cap_{D \in W} D]$. Then $f(x) = y$ for some element **y** belonging to $\cap_{D \in W} D$, so that $y \in D$ for each $D \in W$. Therefore we have $x \in f^{-1}[D]$ for each $D \in W$, which means that **x** belongs to $\cap_{D \in W} f^{-1}[D]$, and this proves one containment direction. Conversely, suppose $x \in \cap_{D \in W} f^{-1}[D]$. Then by definition we know that $f(x) \in D$ for every $D \in W$, so that we must also have $f(x) \in \cap_{D \in W} D$. But this means that $x \in f^{-1}[\cap_{D \in W} D]$, proving containment in the other direction; it follows that the two sets under consideration must be equal.

Verification of **(6):** If $y \in f[f^{-1}[D]]$, then $y = f(x)$ for some $x \in f^{-1}[D]$, and by definition of the latter we know that $f(x) \in D$; since $y = f(x)$ this means that **y** must belong to **D**, proving the containment assertion.

Verification of **(7):** Suppose first that $x \in f^{-1}[B - D]$. By definition $f(x) \in B - D$, and in particular it follows that $f(x) \notin D$, so that $x \notin f^{-1}[D]$. The latter in turn implies that $x \in A - f^{-1}[D]$, and thus we have established $f^{-1}[B - D] \subset A - f^{-1}[D]$. Conversely, if $x \in A - f^{-1}[D]$, then $x \notin f^{-1}[D]$ implies $f(x) \notin D$, so that $f(x) \in B - D$ and hence $x \in f^{-1}[B - D]$. This yields containment in the other direction. ■

Notes. In the next section, we shall prove that equality holds for parts **(3)** and **(6)** if the function **f** satisfies an additional condition (there are separate ones for each part). Likewise, there are results for comparing **f [A – C]** to **B – f [C]** in some cases (see Exercise **IV.4.7**).

Some fundamental constructions

This subsection contains two loosely related comments about the use of set theory and functions to formalize some fundamental mathematical concepts.

Multivariable functions. Frequently in mathematics and its applications one encounters so – called *functions of several variables*. Formally, a function which depends upon **n** independent variables in the sets $\mathbf{A_1, \ldots, A_n}$ is defined to be a function on the **n** – fold Cartesian product

$$\mathbf{A_1 \times \ldots \times A_n}$$

or some subset of such a product. Of course, multivariable calculus provides many examples of functions of 2 and 3 variables where each set $\mathbf{A_i}$ is the real numbers and the codomain is also the real numbers.

Binary operations and algebraic systems. One can also use functions to give a formal definition of algebraic operations on a set. Specifically, if **A** is a set and $*$ is a binary operation on **A**, then one formalizes this operation mathematically by means of a function $\mathbf{b : A \times A \to A}$. Given such an operation we usually denote the value **b(x, y)** in the simpler and more familiar form $\mathbf{x * y}$. In particular, if **A** is the real numbers then addition and multiplication correspond to functions of two variables

$$\alpha : \mathbf{A \times A \to A} \qquad \mu : \mathbf{A \times A \to A}$$

whose values satisfy appropriate conditions.

Similarly, if we are given a mixed binary operation like scalar multiplication, which sends a scalar c and a vector **v** to the vector $c\mathbf{v}$, we can formalize such an operation as a function $\mathbf{C \times A \to A}$. Likewise, an inner product on a vector space corresponds to a function of the form $\mathbf{A \times A \to B}$, where **A** is the vector space and **B** denotes the associated set of scalars. One can even go further and discuss binary operations like matrix multiplications which send an $m \times n$ matrix and an $n \times p$ matrix to an $m \times p$ matrix, and in such cases the binary operations will be mappings $\mathbf{A \times B \to C}$, where the three sets **A**, **B** and **C** may all be distinct.

A problem involving polar coordinates

Many intermediate or advanced treatments of polar coordinates contain a section on finding the intersection points of two plane curves given in polar coordinates. If the curves are defined by equations of the form $\mathbf{F(r, \theta) = 0}$ and $\mathbf{G(r, \theta) = 0}$, then some points of this type are given by the values of $\mathbf{(r, \theta)}$ which solve both of these equations, but *frequently one encounters examples where this does* ***not*** *yield* ***all*** *the common*

points. One example of this sort is given by the circle with equation $r = 1$ and the line with equation $\theta = 1$. The common solutions of the two equations yield the point in the plane with polar coordinates $(1, 1)_{POLAR}$, but if one graphs the two curves it is also apparent that $(-1, 1)_{POLAR} = (1, 1 + \pi)_{POLAR}$ is also on both curves.

Sometimes calculus texts address this difficulty by suggesting that one graph the two curves to see if there are any common points that are not given by simultaneous solutions of the equations. This is usually effective, but it is neither systematic nor logically complete. We shall use the material developed thus far in this course to give a more reliable basis for finding common points. Additional details appear in the following online document:

http://math.ucr.edu/~res/math9C/polar-ambiguity.pdf

In fact, we shall look at an abstract version of the polar coordinate problem. Suppose that we are given a surjective function $f : A \to B$ be from one set **A** to a second set **B**; in the special case of immediate interest, the sets **A** and **B** are both equal to the real numbers and **f** is the standard polar coordinate map sending (r, θ) to $(r \cos \theta, r \sin \theta)$. What is the abstract version of two curves C_1 and C_2 defined by equations in polar coordinates? The equations have the form $g_1(a) = x_1$ and $g_2(a) = x_2$ for functions $g_1, g_2 : A \to X$, and the abstract versions of C_1 and C_2 are the set of all points $b \in B$ such that there are some $a \in A$ satisfying $f(a) = b$ and $g_1(a) = x_1$ (for C_1) or $f(a) = b$ and $g_2(a) = x_2$ (for C_2). This intersection includes all points $b \in B$ such that there is some $a \in A$ satisfying $f(a) = b$, $g_1(a) = x_1$ and $g_2(a) = x_2$. However, the following result, which is elementary to verify, describes **ALL** the possibilities:

Proposition 3. *In the setting of the preceding paragraph, the intersection* $C_1 \cap C_2$ *consists of all* $b \in B$ *for which there exist* $a_1, a_2 \in A$ *such that* $f(a_1) = f(a_2) = b$, $g_1(a) = x_1$, *and* $g_2(a) = x_2$.■

Application to the previous example. In this case the equations $g_1(a) = x_1$ and $g_2(a) = x_2$ are $r - 1 = 0$ and $q - \theta = 0$. We then have $f(-1, 1) = f(1, 1 + \pi)$, and we also have $g_1(-1, 1) = 0 = g_2(1, 1 + \pi)$. Therefore the criterion in the proposition implies that $f(-1, 1) = f(1, 1 + \pi) \in C_1 \cap C_2$. Graphically it is clear that this point and $f(-1, 1)$ are the only points at which the line and circle meet, but we need to check this analytically in order to be logically complete. Given (r, θ), the definition of polar coordinates shows that $f(r, \theta) = f(s, \varphi)$ if and only if either (1) $r = s = 0$ and the second coordinate is arbitrary, (2) $s = (-1)^m r$ and $\varphi = \theta + \pi m$. No coordinate pairs (r, θ) and (s, φ) the first type yield solutions as in the proposition, and in the situation we are considering it is elementary to check that no additional common points arise from coordinate pairs of the second type.

IV.4: Composite and inverse functions

(Halmos, § 10; Lipschutz, §§ 4.3 – 4.4, 5.7)

This section discusses two basic methods of constructing new functions from old ones. Both play an important role in calculus.

1. The formation of ***composites*** by taking a function of a function. For example, the composite of $\sin x$ and $2x + 1$ is the function $\sin(2x + 1)$, and the composite of the functions $1 + x^3$ and e^x is equal to $1 + e^{3x}$.
2. In some situations, it is possible to undo the results of a function by taking the ***inverse*** function. For example, the cube root function is the inverse of x^3, the natural logarithm function is the inverse of e^x, and $\arctan x$ is the inverse to $\tan x$ if the latter is viewed as a function which is defined on the open interval $(-\pi/2, \pi/2)$.

Identity and composite functions

As noted above, one standard method for constructing new functions out of old ones is to compose them. In particular, if **f** and **g** are suitable functions, then one can form the composite $g(f(x))$ by first applying **f** to **x** and then applying **g** to the resulting value **f(x).** In order for this to be defined the value **x** must be in the domain of **f,** and **f(x)** must be in the domain of **g.** For example**,** over the real numbers one cannot form the composite function $\mathrm{sqrt}(\sin x - 2)$ because the expression inside the radical sign is always negative and in elementary calculus one can only define square roots for nonnegative numbers**.**

Formally, we proceed as follows**:**

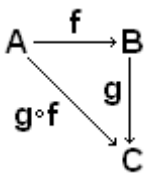
Definition. If $f : A \to B$ and $g : B \to C$ are functions, then the ***composite function***

$$g \circ f : A \to C$$

is defined by $g \circ f(x) = g(f(x))$. Frequently one abbreviates $g \circ f$ to gf.

Example. Suppose that $f(x) = 7x - 4$ and $g(x) = 3x + 2$. Then direct calculation shows that $g \circ f(x) = 21x - 10$.

Graphically one often represents a composite by a so – called ***commutative diagram***, the idea being that if one follows the arrows from one object to another, the end result is independent of the path taken.



During the past half century the use of commutative diagrams has become extremely widespread in the mathematical sciences and in some closely related areas (***e.g.*****,** some branches of theoretical physics)**.** Section 5.6 of Lipschutz contains some further discussion of this point**.**

Composition of functions is associative but not commutative. We shall establish the first by proving a proposition and the second by furnishing an example**.**

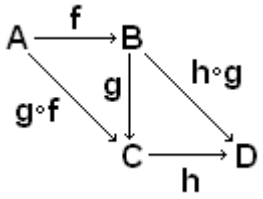
Proposition 1. *Suppose that* $f: A \to B$, $g: B \to C$, *and* $h: C \to D$ *are functions. Then we have the associativity identity* $h \circ (g \circ f) = (h \circ g) \circ f$.

Proof. This follows directly from the definition of functional composition. If $x \in A$ is arbitrary, then we have the chain of equations

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x).$$

By Proposition 1 it follows that the two composites $h \circ (g \circ f)$ and $(h \circ g) \circ f$ must be equal**.**■

The proof may be illustrated by the following commutative diagram



in which each of the two triangles ΔABC, ΔBDC commutes; it follows from associativity that the parallelogram $\square ABDC$ also commutes**.**

Failure of commutativity. One basic reason why composition is not commutative **(*i.e.*,** $g \circ f \neq f \circ g$ in general**)** is that the existence of one of the composites $g \circ f$ or $f \circ g$ does not guarantee the existence of the other**.** For example**,** this happens whenever we have $f: A \to B$ and $g: B \to C$ where **A, B** and **C** are all distinct**.** In particular, in order to define both composites we need to have $A = C$**,** and if **B** is not equal to **A** there is still no way that $g \circ f$ or $f \circ g$ can be equal because they still have different domains and codomains**.** Thus the only remaining situations in which one can ask whether the composites in both orders are equal are those where $A = B = C$**.** The example below shows that commutativity fails even in such a restricted setting.

Examples. **1.** Let $A = B$ be the real numbers, let $f(x) = x + 3$**,** and let $g(x) = x^2$**.** Then the composite $g \circ f(x)$ is equal to $(x + 3)^2$**,** but the reverse composite $f \circ g(x)$ is equal to $x^2 + 3$**.** so that $g \circ f$ and $f \circ g$ are completely different functions**.** In particular**,** their values for $x = 0$ are unequal**.**

2. Consider the functions $f(x) = x + 1$ and $g(x) = x^3$**.** Both **f** and **g** are **1 – 1** onto functions from the real numbers to themselves**,** but $g \circ f(x) = x^3 + 1$ while the composite in the other order given by $f \circ g(x) = (x + 1)^3 = x^3 + 3x^2 + 3x + 1$**.**

3. If we take $f(x) = \sin x$ and $g(x) = x^2$**,** then both **f** and **g** are functions from the real numbers to themselves with $g \circ f(x) = \sin^2 x$ and $f \circ g(x) = \sin(x^2)$**.** Note that the

first of these has an antiderivative that is easily expressed in terms of elementary functions from single value calculus but the second does not; more information on the latter topic appears in the document

http://math.ucr.edu/~res/math144/nonelementary_integrals.pdf

in the course directory**.**

Composition, images and inverse images. The image and inverse image constructions are highly compatible with composition of functions.

Proposition 2. *Suppose that* $f: A \to B$ *and* $g: B \to C$ *are functions, and let* M *and* N *denote subsets of* A *and* C *respectively. Then we have*

$$g \circ f\,[M] = g[\,f[M]\,] \qquad \textit{and} \qquad (g \circ f)^{-1}[N] = f^{-1}[\,g^{-1}[N]\,].$$

Proof. We shall first verify that $g \circ f\,[M] = g[f[M]]$. Suppose that $z = g \circ f(x)$ for some $x \in M$. Since $(g \circ f)(x) = g(f(x))$ it follows that we have $z = g(y)$ where $y = f(x)$ and $x \in M$. Therefore $y \in f[M]$ and consequently we also have $z \in g[f[M]]$. To prove the reverse inclusion, suppose that $z \in g[f[M]]$, so that $z = g(y)$ where $y = f(x)$ and $x \in M$. We may then use $(g \circ f)(x) = g(f(x))$ to conclude that $z \in g \circ f\,[M]$, completing the proof of the second inclusion and thus also the proof that the two sets under consideration are equal.

We shall next verify that $(g \circ f)^{-1}[N] = f^{-1}[g^{-1}[N]]$. Suppose that x belongs to the set $(g \circ f)^{-1}[N]$. By definition we then have $g \circ f(x) \in N$, and since $(g \circ f)(x) = g(f(x))$ it follows that $f(x) \in g^{-1}[N]$. The latter in turn implies that $x \in f^{-1}[\,g^{-1}[N]\,]$, and this proves containment in one direction. To prove containment in the other direction, suppose that $x \in f^{-1}[\,g^{-1}[N]\,]$. Working backwards, we conclude that $f(x) \in g^{-1}[N]$, so that $(g \circ f)(x) = g(f(x)) \in N$, which implies that $x \in (g \circ f)^{-1}[N]$. This proves containment in the other direction and hence that the two sets under consideration are equal.■

Definition. Given a set A, the ***identity function*** id_A or $1_A : A \to A$ is the function whose graph is the set of all (x, y) such that $y = x$.

Identity maps and composition of functions satisfy the following simple but important condition.

Proposition 3. *If* $f: A \to B$ *is a function, then we have* $1_B \circ f = f = f \circ 1_A$.

Proof. Let $x \in A$ be arbitrary. Then we have $1_B \circ f(x) = 1_B(f(x)) = f(x)$ and we also have $f(x) = f(1_A(x)) = f \circ 1_A(x)$. We can now apply Proposition IV.3.1 to conclude that the three functions $1_B \circ f$, f, and $f \circ 1_A$ are equal.■

Inclusion mappings. If A is a set and C is a subset of A, then the *inclusion* mapping $j: C \to A$ is the function defined by $j(x) = x$; equivalently, the graph is the set of all (x, y) in $C \times A$ such that $x = y$.

Restrictions to subsets. Suppose that $\mathbf{f: A \to B}$ is a function, and again let **C** be a subset of **A.** Then the *restriction of* **f** *to* **C** is the composite function $\mathbf{f \circ j: C \to B}$, and it is generally denoted by $\mathbf{f|C}$. If the graph of **f** is the set $\mathbf{G \subset A \times B}$, then the graph of $\mathbf{f|C}$ is the subset $\mathbf{G \cap (C \times B)}$.

Special types of functions

Defintions. Let $\mathbf{f : A \to B}$ be a function.

- The function **f** is *one – to – one* or **1 – 1** if for all $\mathbf{x, y \in A}$, we have $\mathbf{f(x) = f(y)}$ if and only if $\mathbf{x = y}$. Such a map is also said to be *injective* or an *injection* or a *monomorphism* or an *embedding* (sometimes also spelled *imbedding*).
- The function **f** is *onto* if for each $\mathbf{y \in B}$ there is some $\mathbf{x \in A}$ such that $\mathbf{f(x) = y}$. Such a map is also said to be *surjective* or a *surjection* or an *epimorphism*.
- The function **f** is **1 – 1** *and onto* (or **1 – 1** *onto* or a **1 – 1** *correspondence*) if it is both **1 – 1** and onto. Such a map is also said to be *bijective* or a *bijection* or an *isomorphism*.

The following observation is a direct consequence of the definitions.

Proposition 4. *Let* $\mathbf{f : A \to B}$ *be a function. Then* **f** *is surjective if and only if its range is equal to its codomain, or equivalently if and only if* $\mathbf{f[A] = B}$.■

This follows immediately because the range of **f** is equal to **f [A]** by definition.

Examples of injections. If **A** is a set and **C** is a subset of **A,** then the previously defined inclusion mapping $\mathbf{j: C \to A}$ is an injection because $\mathbf{j(x) = x}$ for all **x,** so that the condition $\mathbf{j(x) = j(y)}$ is equivalent to saying that $\mathbf{x = y}$. On the other hand, the inclusion **j** is a surjection if and only if $\mathbf{C = A}$.

Examples of surjections. Let **A** and **B** be sets, and let $\mathbf{A \times B}$ denote their Cartesian product. The ***(coordinate) projection mappings*** $\mathbf{p_A : A \times B \to A}$ and $\mathbf{p_B : A \times B \to B}$ ***onto*** **A** and **B** respectively are defined by $\mathbf{p_A(x, y) = x}$ and $\mathbf{p_B(x, y) = y}$. These are also called the ***projections onto the first*** **(A –)** ***and second*** **(B –)** ***coordinates***. If both **A** and **B** are nonempty, then these mappings are always surjective. On the other hand, the projection $\mathbf{p_A}$ is injective if and only if **B** consists of a single point, and likewise the projection $\mathbf{p_B}$ is injective if and only if **A** consists of a single point.

Additional examples for injectivity and surjectivity. Injectivity and surjectivity are logically independent properties. The standard way of showing this is to give an example of a function that is injective but not surjective and an example that is surjective but not injective. For the former, consider the elementary function $\mathbf{f : \mathbb{R} \to \mathbb{R}}$ defined by $\mathbf{f(x) = \arctan x}$. This is defined for all numbers and is strictly increasing, so it is automatically ***injective, but it is not surjective*** because its range is the open interval $\mathbf{(-\pi/2, \pi/2)}$. An example of a function that is ***surjective but not injective*** is given by $\mathbf{f(x) = x^3 - x}$. The function is surjective because for each **y** one can find a real solution to the cubic equation $\mathbf{x^3 - x = y}$. However, it is not injective because $\mathbf{f(0) = f(+1) = f(-1) = 0}$.■ Note also that the function $\mathbf{f(x) = x^2}$ is ***neither injective nor surjective*** because $\mathbf{f(+1) = f(-1)}$ and it is not possible to find a real number **x** such that $\mathbf{x^2 = -1}$. ■

The following simple factorization principle turns out to be extremely useful for many purposes**:**

Proposition 5. *Let* $\mathbf{f : A \to B}$ *be a function. Then* **f** *is equal to a composite* $\mathbf{j \circ q}$**,** *where* $\mathbf{q: A \to C}$ *is surjective and* $\mathbf{j : C \to B}$ *is injective*.

Proof. Let **C** be the image of **f,** and define **q** such that the graphs of **q** and **f** are equal. Take **j** to be the inclusion of **C** in **B** (hence it is injective). By construction **q** is surjective, and it follows immediately that $\mathbf{f(x) = j(\, q(x)\,)}$ for all **x** in **A.**■

Note. The factorization of a function into a surjection followed by an injection is rarely unique, but there is a close relationship between any two such factorizations whose proof is left to the exercises for this section**.**

Complement to Proposition 5. Suppose we have a function $\mathbf{f : A \to B}$ and two factorizations of **f** as $\mathbf{j_0 \circ q_0}$ and $\mathbf{j_1 \circ q_1}$ where the maps $\mathbf{q_t}$ are surjective and the maps $\mathbf{j_t}$ are injective for $\mathbf{t = 0, 1.}$ Denote the codomain of $\mathbf{q_t}$ (equivalently, the domain of $\mathbf{j_t}$) by $\mathbf{C_t}$**.** Then there is a unique bijection $\mathbf{H: C_0 \to C_1}$ such that $\mathbf{H\, q_0 = q_1}$ and $\mathbf{j_1\, H = j_0}$**.** A wide range of injective**,** surjective and bijective functions arise in subjects like calculus, discrete mathematics and linear algebra**.** The reader is encouraged to look back at various basic functions from such courses to determine which if any of these conditions are satisfied for such examples**.**

Proposition 6. *Let* $\mathbf{f: A \to B}$ *and* $\mathbf{g: B \to C}$ *be functions.*

- **(1)** *If* **f** *and* **g** *are surjections then so is* $\mathbf{g \circ f}$**.**
- **(2)** *If* **f** *and* **g** *are injections then so is* $\mathbf{g \circ f}$**.**
- **(3)** *If* **f** *and* **g** *are bijections, then so is* $\mathbf{g \circ f}$**.**

Proof. The third statement follows from the first two**,** so it suffices to prove these assertions.

Verification of **(1):** Assume **f** and **g** are onto**.** Let $\mathbf{c \in C}$ be arbitrary**.** Since **g** is onto we can take $\mathbf{b \in B}$ such that $\mathbf{g\,(b) = c.}$ Since **f** is onto there is some $\mathbf{a \in A}$ such that $\mathbf{f\,(a) = b.}$ But then $\mathbf{g \circ f\,(a) = g\,(\,f(a)\,) = g\,(b) = c.}$ Hence $\mathbf{g \circ f}$ is onto**.**

Verification of **(2):** Assume **f** and **g** are $\mathbf{1 - 1.}$ Take arbitrary elements $\mathbf{a_1, a_2 \in A}$ and suppose that $\mathbf{g \circ f(a_1) = g \circ f(a_2).}$ Then $\mathbf{g(f(a_1)\,) = g(\,f(a_2))}$ by the definition of the composite $\mathbf{g \circ f.}$ Therefore $\mathbf{f(a_1) = f(a_2)}$ because **g** is $\mathbf{1 - 1,}$ and since **f** is $\mathbf{1 - 1}$ it now follows next that $\mathbf{a_1 = a_2.}$ This shows that $\mathbf{g \circ f}$ is $\mathbf{1 - 1.}$■

If a function $\mathbf{f: A \to B}$ is either $\mathbf{1 - 1}$ or onto, then one can prove strengthened forms for some of the results in Theorem IV.3.2 on images and inverse images of subsets with respect to **f.**

Theorem 7. *If* $\mathbf{f : A \to B}$ *is a function, then the image and inverse image constructions for* **f** *have the following properties***:**

1. *If* **f** *is* $\mathbf{1 - 1}$ *and* **C** *is a subset of* **A,** *then* $\mathbf{C = f^{-1}[f[C]].}$
2. *If* **f** *is onto and* **D** *is a subset of* **B,** *then* $\mathbf{f\,[f^{-1}[D]] = D.}$

Proof. As in the proof of Theorem $\mathbf{IV.3.2,}$ we treat each statement separately**.**

Verification of **(1):** By Theorem **IV.3.2,** we already know **C** is contained in $\mathbf{f^{-1}[f[C]]}$. Suppose now that **f** is $\mathbf{1-1}$ and $\mathbf{y \in f^{-1}[\,f[C]]}$. By definition we know that **f(y) = f(x)** for some $\mathbf{x \in C}$. Since **f** is $\mathbf{1-1}$ this implies **y = x,** so that we must have $\mathbf{x \in C}$. Hence the two sets under consideration are equal if **f** is $\mathbf{1-1}$.

Verification of **(2):** By Theorem **IV.3.2,** we already know $\mathbf{f\,[f^{-1}[D]\,]}$ is contained in **D.** Suppose now that **f** is onto, and let $\mathbf{y \in D}$. Then there is some **x** such that **y = f(x),** and by definition we know that **x** must belong to $\mathbf{f^{-1}[D]}$. Therefore **y = f(x)** must belong to $\mathbf{f[\,f^{-1}[D]]}$ if **f** is onto, proving containment in the other direction if **f** is onto.■

Inverse functions

Intuitively, the inverse of a function $\mathbf{f: A \to B}$ is a function $\mathbf{g: B \to A}$ which undoes the action of **f;** frequently we say that a function is ***invertible*** if an inverse exists. It turns out that a function is only invertible if it is a bijection.

Definition. Let $\mathbf{f: A \to B}$ be a function. A function $\mathbf{g: B \to A}$ which is an ***inverse*** of **f** if for all $\mathbf{a \in A}$ we have $\mathbf{g\,(f(a)) = a}$ and for all $\mathbf{b \in B}$ we have $\mathbf{f\,(g(b)) = b}$. This is clearly equivalent to the conditions $\mathbf{g \circ f = id_A}$ and $\mathbf{f \circ g = id_B}$.

Elementary examples. If **A** denotes the real numbers, **B** denotes the positive real numbers, and $\mathbf{f(x) = e^x}$, then **f** has an inverse function **g** which is the logarithm of **x** to the base **e.** Similarly, if **A = B** is the real numbers and **f(x) = 2x + 4,** then **f** has an inverse **g** and **g(x) = ½x – 2.** Many other examples of this sort arise in trigonometry and calculus.

Proposition 8. *Let* $\mathbf{f: A \to B}$ *be a bijection, and define* $\mathbf{f^{-1}: B \to A}$ *by taking* $\mathbf{f^{-1}(b)}$ *to be the unique a such that* **f (a) = b;** *equivalently, the graph of* $\mathbf{f^{-1}}$ *is the set of all ordered pairs* **(y, x)** *such that* **(x, y)** *lies in the graph of* **f.** *Then* $\mathbf{f^{-1}}$ *is well-defined, and it is an inverse of* **f** *(in fact it is the* ***unique*** *inverse in view of the next proposition).*

Proof. There is at least one a such that **f (a) = b** since **f** is onto. There cannot be more than one since **f** is $\mathbf{1-1}$. Therefore $\mathbf{f^{-1}}$ is well – defined. It clearly satisfies the conditions for being an inverse of **f.**■

Proposition 9. *Let* $\mathbf{f: A \to B}$ *be a function. If* **f** *has an inverse* **g,** *then* **f** *is a bijection and the inverse is unique (and it is equal to* $\mathbf{f^{-1}}$ *as defined above).*

Proof. Assume that the mapping **f** has an inverse **g.** To show that **f** is onto, take $\mathbf{b \in B}$. Then **f(g(b)) = b,** so **b** lies in the image of **f.** To show that **f** is $\mathbf{1-1}$, consider an arbitrary pair of elements $\mathbf{a_1, a_2 \in A}$. Suppose that $\mathbf{f(a_1) = f(a_2)}$. Then $\mathbf{g(\,f(a_1)\,) = g(\,f(a_2)\,)}$, and since $\mathbf{g \circ f}$ is the identity it follows that $\mathbf{a_1 = a_2}$. To show that the inverse is unique, suppose that **g** and **h** are both inverses of **f.** We must show that **g = h.** Let $\mathbf{b \in B}$ be arbitrary. Then $\mathbf{f(\,g(b)\,) = f(\,h(b)\,) = b}$ because **g** and **h** both inverses, and since **f** is $\mathbf{1-1}$ we must have **g(b) = h(b)** for all **b.** By Proposition **3.1,** we have shown that **g = h.**■

In view of the preceding proposition, one way of showing that a function is a bijection is to show that it has an inverse.

The construction sending a bijective function to its inverse has several basic properties that are summarized in the next result.

Proposition 10. *The inverse construction has the following properties:*

1. *Let* $\mathbf{A}$ *be a set. Then the identity map* $\mathbf{id}_A$ *is a bijection, and it is equal to its own inverse.*
2. *Suppose that* $\mathbf{f: A \to B}$ *and* $\mathbf{g: B \to C}$ *are bijections so that their composite* $\mathbf{g \circ f}$ *is also a bijection by a previous result. Then the function* $\mathbf{(g \circ f)^{-1}}$ *is equal to* $\mathbf{f^{-1} \circ g^{-1}}$.
3. *If* $\mathbf{f: A \to B}$ *is a bijection with inverse* $\mathbf{f^{-1}}$, *then* $\mathbf{f^{-1} : B \to A}$ *is also a bijection, and its inverse is equal to* $\mathbf{f}$.

Proof. We shall derive all of these from the conditions $\mathbf{v \circ u = id_X}$ and $\mathbf{u \circ v = id_Y}$ which characterize a function $\mathbf{u : X \to Y}$ and its inverse $\mathbf{v : Y \to X}$. If $\mathbf{u = id_A}$ then we also have $\mathbf{v = id_A}$ because $\mathbf{id_A \circ id_A = id_A}$, proving the first part. To prove the second part, we take $\mathbf{X = A,\ Y = C}$, and $\mathbf{u = g \circ f}$. If we set $\mathbf{v}$ equal to $\mathbf{f^{-1} \circ g^{-1}}$, then Propostion 1 (the associativity property for compositions) and Proposition 3 (on composites with identity maps) combine to imply that the composites $\mathbf{v \circ u}$ and $\mathbf{u \circ v}$ are both identity maps. Finally, if $\mathbf{X = B,\ Y = A}$, and $\mathbf{u = f^{-1}}$, then $\mathbf{v = f}$ has the property that the composites $\mathbf{v \circ u}$ and $\mathbf{u \circ v}$ are both identity maps. ■

Example. Here is an illustration of the identity $\mathbf{(g \circ f)^{-1} = f^{-1} \circ g^{-1}}$ using the functions $\mathbf{f : \mathbb{R} \to \mathbb{R}}$ defined by $\mathbf{f(x) = e^x}$ and $\mathbf{g : \mathbb{R} \to (0,\ 1)}$ defined by $\mathbf{g(y) = y/(1+y)}$ as examples for the composite formula for inverse functions: The composite $\mathbf{g \circ f}$ is given by $\mathbf{z = e^x/(1 + e^x)}$, and if we solve for $\mathbf{z}$ we get the equation $\mathbf{x = \ln (z/(1 - z))}$. Since $\mathbf{g^{-1}(z)}$ is equal to the expression inside the parentheses and $\mathbf{\ln y = x}$ is the inverse to $\mathbf{y = e^x}$, this example does satisfy the formula for finding the inverse function of a composite. ■

The Axiom of Replacement

We have repeatedly noted that sets are supposed to be classes that are "reasonably small." Such a viewpoint suggests that if $\mathbf{A}$ is a set and $\mathbf{B}$ is a class that can be put into a $\mathbf{1 - 1}$ correspondence with $\mathbf{A}$, then $\mathbf{B}$ should also be a set. The following stronger axiom confirms this intuitive conclusion:

AXIOM OF REPLACEMENT. *Let* $\mathbf{P(- , -)}$ *be a two variable predicate statement such that for each set* $\mathbf{x}$ *there is a unique set* $\mathbf{y}$ *such that* $\mathbf{P(x, y)}$ *is true. Then for each set* $\mathbf{A}$, *the collection* $\mathbf{P[\ A\ , - \ ]}$ *of all* $\mathbf{y}$ *such that* $\mathbf{P(x, y)}$ *for some* $\mathbf{x \in A}$ *is a set.*

Background information and the reasons for exactly this statement are summarized on pages 92 – 102 of the book by Goldrei which is cited at the beginning of the Unit **I** of these notes.

For our purposes the most important special cases arise when **P(x, y)** is a statement that $\mathbf{x} \in \mathbf{A}$ for some set **A** and $\mathbf{y} \in \mathbf{B}$ for some set **B,** and the statement **P(x, y)** asserts that **(x, y)** lies in some subclass Γ of $\mathbf{A} \times \mathbf{B}$. For such examples the axiom has the following implication**:**

Corollary 11. *Suppose that* **A** *is a set,* **B** *is a class and* Γ *is a subclass of* $\mathbf{A} \times \mathbf{B}$ *such that for each* $\mathbf{a} \in \mathbf{A}$ *there is a unique element* $\mathbf{b} \in \mathbf{B}$ *such that* $(\mathbf{a}, \mathbf{b}) \in \Gamma$. *Then the collection of all* $\mathbf{b} \in \mathbf{B}$ *such that* $(\mathbf{a}, \mathbf{b}) \in \Gamma$ *for some* $\mathbf{a} \in \mathbf{A}$ *is a set.*■

In less formal terms**,** if we are given a set **A** and something which looks like a function on **A,** then the class that should be the image of **A** is also a set**.** If we further specialize to subclasses Γ such that for each $\mathbf{b} \in \mathbf{B}$ there is a unique $\mathbf{a} \in \mathbf{A}$ such that $(\mathbf{a}, \mathbf{b}) \in \Gamma$**,** then we obtain the conclusions in the first sentence of this subsection**;** ***i.e.*****.,** if we know that a class **B** is in $\mathbf{1-1}$ correspondence with a set **A,** then **B** is also a set**.**

IV.5: Constructions involving functions

(Halmos, § 8; Lipschutz, § 5.7)

This section discusses two unrelated points**.** The first concerns an important relationship between equivalence relations and surjective functions**,** and the second describes some basic facts about the collection of all functions from one set to another**.**

Equivalence relations and quotient projections

We have already mentioned that functions are at least as fundamental to mathematics as sets and that most if not all of set theory can be reformulated in terms of functions. The application of this principle to equivalence relations is particularly important. Let **A** be a set, let ***E*** be an equivalence relation on **A**, and let $\mathbf{A}/\boldsymbol{E}$ be the set of equivalence classes for ***E*****.** One then has an associated ***quotient projection***

$$\Pi_{\boldsymbol{E}} : \mathbf{A} \to \mathbf{A}/\boldsymbol{E}$$

defined by the formula $\Pi_{\boldsymbol{E}}(\mathbf{x}) = [\mathbf{x}]_{\boldsymbol{E}}$ (***i.e.*****.,** an element **x** is sent to its ***E*** – equivalence class). By construction the map $\Pi_{\boldsymbol{E}}$ is always onto, and it is $\mathbf{1-1}$ if and only if each equivalence class consists of exactly one element (hence the equivalence relation in question is just equality)**.**

The discussion of the preceding paragraph shows that an equivalence relation defines a function**;** conversely**,** the discussion below shows that every function defines an equivalence relation**.**

Definition. Let **f: A → B** be a function**.** Define a binary relation ***F*** on **A** such that **x *F* y** if and only if **f(x) = f(y).**

Proposition 1. *In the setting above, the relation **F** is an equivalence relation***.**

Proof. The condition **x *F* x** is a trivial consequence of **f(x) = f(x).** Given **x *F* y,** by definition we have **f(x) = f(y),** which is equivalent to **f(y) = f(x)** and thus implies **y *F* x.** If **x *F* y** and **y *F* z,** then we have **f(x) = f(y)** and **f(y) = f(z),** so that **f(x) = f(z)** and hence **x *F* z.** Therefore ***F*** is an equivalence relation**.**

By construction**,** the equivalence classes of ***F*** are in $\mathbf{1-1}$ correspondence with the elements of the image **f [A].**■

The following result on functions and equivalence relations is extremely useful in certain situations**.**

Theorem 2. *Let* **f: A → B** *be a function, and let **E** be an equivalence relation on* **A** *such that* **f (x) = f (y)** *whenever* **x *E* y.** *Then there is a unique function* **g : A/*E* → B** *such that* **f = g ∘ Π_E.**■

Proof. **(**)** Let **w ∈ A/*E*** and choose **x ∈ A** representing the equivalence class **w.** We would like to set **g(w)** equal to **f(x),** but in order to do so it is necessary to verify that the latter does not depend upon the choice of representative**.** Suppose that **y** also represents **w,** so that **x *E* y.** It then follows from the hypothesis that **f (x) = f (y)** and therefore the construction **g(w) = f(x)** does determine a well – defined function from **A/*E*** to **B.** Furthermore**,** by construction we have **f = g ∘ Π_E.** This proves existence. To prove uniqueness**,** suppose that **h** is an arbitrary function such that **f = h ∘ Π_E.** Let **w ∈ A/*E*** and **x ∈ A** be arbitrary elements such that **x** represents **w;** by Proposition 3.1 (the criterion for functions to be equal) it suffices to show that **g(w) = h(w)** for every **w.** By construction we have **w = Π_E(x),** and therefore by our assumptions and construction we have

$$\mathbf{g(w) = g \circ \Pi_E(x) = f(x) = h \circ \Pi_E(x) = h(w)}$$

so that **h = g;** this completes the proof of uniqueness**.**■

The following result will be useful for the one of the exercises in Section $\mathbf{V.1.}$

Proposition 3. *Let* **X** *and* **Y** *be sets, let* **f: X → Y** *be a function, let **R** be a binary relation on* **X,** *and let **E** be the equivalence relation generated by **R**. Suppose that for all* **u, v ∈ X** *we know that* **u *R* v** *implies* **f(u) = f(v).** *Then for all* **x, y ∈ X** *such that* **x *E* y** *we also have* **f(x) = f(y).**

Proof. Let ***E*(f)** be the equivalence relation defined by **z *E*(f) w** if and only if **f(z) = f(w).** Then by our assumptions we know that **u *R* v** implies **u *E*(f) v,** so that ***E*(f)** is an equivalence relation containing ***R*.** However, we also know that ***E*** is the unique smallest equivalence relation containing ***R*,** and therefore we must have ***E* ⊂ *E*(f),** which means that **x *E* y** implies **x *E*(f) y.** Since the latter is true if and only if **f(x) = f(y),** this proves the assertion in the proposition**.**■

Sets of functions

One basic principle running throughout this unit is that reasonable constructions on sets within the framework of set theory should yield new examples of sets. Thus far we have done this mainly by means of axioms. However, we have reached a point where our axioms are strong enough to guarantee that still other constructions also yield sets. The following result contains one fundamental example of this type.

Proposition 4. *Suppose that* **A** *and* **B** *are sets. Then the collection of all functions from* **A** *to* **B** *is also a set.*

Proof. By definition a function from **A** to **B** consists of an ordered pair whose first coordinate is **(A, B)** and whose second coordinate is a subset of $\mathbf{A \times B}$. This means that a function is an element of the set $(\{\mathbf{A}\} \times \{\mathbf{B}\}) \times \mathbf{P(A \times B)}$. Since a subclass of a set is a set, this proves that the collection of functions is a set.■

Notation. If **A** and **B** are sets, then the set of all functions from **A** to **B** is denoted by $\mathbf{B^A}$.

Sets of functions play an important role in many mathematical contexts. We shall only discuss one of them, after which we shall mention some of their basic formal properties without proofs (none of these results will be needed later in the course).

Proposition 5. *If* **A** *is a set, then there is a* $\mathbf{1-1}$ *correspondence from* **P(A)** *to the set of functions* $\mathbf{\{0,1\}^A}$.

Remark on terminology. The existence of this $\mathbf{1-1}$ correspondence is the underlying reason why **P(A)** is often called the ***power set*** of **A.**

Proof. Let **B** be a subset of **A,** and define the ***indicator function*** or ***characteristic function*** $\mathbf{J_B : A \to \{0, 1\}}$ by $\mathbf{J_B(x) = 1}$ if $\mathbf{x \in B}$ and $\mathbf{J_B(x) = 0}$ if $\mathbf{x \notin B}$. Since the set of points where $\mathbf{J_B(x) = 1}$ is equal to **B,** it follows that $\mathbf{J_B \neq J_C}$ if $\mathbf{B \neq C}$. Thus the map $\mathbf{J : P(A) \to \{0, 1\}^A}$ is $\mathbf{1-1}$. To see that the map is onto, let $\mathbf{h : A \to \{0, 1\}}$; by construction it follows that $\mathbf{h = J_D}$, where **D** is the set of all points **x** such that $\mathbf{h(x) = 1}$. Therefore **J** is a $\mathbf{1-1}$ correspondence.■

We now describe some formal properties of function sets that are sometimes useful.

Proposition 6. *Composition of functions determines a function*

$$\varphi : \mathbf{B^A \times C^B \to C^A}$$

such that $\varphi(\mathbf{f, g}) = \mathbf{g \circ f}$.

The final result of this subsection justifies the exponential notation for sets of functions by displaying some identities that are formally similar to some basic laws of exponents.

Theorem 7. (Exponential laws) *If* **A, B** *and* **C** *are sets, then there is a* $\mathbf{1-1}$ *correspondence between* $\mathbf{(B \times C)^A}$ *and* $\mathbf{B^A \times C^A}$, *and there is also a* $\mathbf{1-1}$ *correspondence between* $\mathbf{(C^B)^A}$ *and* $\mathbf{C^{B \times A}}$.■

Hints for proving the exponential laws are given in the exercises for this section.

IV.6 : Order types

(Halmos, § 18; Lipschutz, §§ 7.7 – 7.10)

We shall conclude this unit with an application of functions to the study of partially ordered sets**.** The cited section of Halmos begins with material not yet discussed in these notes**,** so we should mention that the relevant material in that reference begins near the bottom of page 71**,** starting with the paragraph**,** "*We continue with an important part of the theory of order*,**"** and ending just before the last paragraph on the next page**.**

In many situations one has two partially ordered sets which have the same basic order-theoretic structure and differ only by a simple change of variable**.** For example**,** the set of nonnegative integers $\mathbb{N}$ and the set $\mathbb{N}^+$ of positive integers have essentially the same order structure**,** and the transition is given by the linear change of variables $\mathbf{y = x + 1.}$ This defines a bijective map $\boldsymbol{\sigma_0}$ from $\mathbb{N}$ to $\mathbb{N}^+$**,** and it has the property that $\mathbf{x \leq x'}$ if and only if $\boldsymbol{\sigma_0}\mathbf{(x) \leq \sigma_0(x').}$ Similarly**,** if **A** and **B** are the sets of positive integers that divide **15** and **14** respectively**,** and each is partially ordered with respect to divisibility, then there is a $\mathbf{1-1}$ correspondence $\mathbf{f : A \to B}$ such that $\mathbf{f(1) = 1,\ f(3) = 2,\ f(5) = 7,}$ and $\mathbf{f(15) = 14,}$ and one can verify directly that

u divides **v** in **A** ***if and only if*** **f(u)** divides **f(v)** in **B.**

More generally**,** we have the following**:**

Definition. Let $\mathbf{(A, \leq_A)}$ and $\mathbf{(B, \leq_B)}$ be partially ordered sets. We say that **A** and **B** are ***similar,*** or ***have the same order type,*** or ***are order – isomorphic,*** if there exists a $\mathbf{1-1}$ correspondence $\mathbf{f : A \to B}$ such that for all $\mathbf{u, v \in A}$ we have $\mathbf{u \leq_A v}$ if and only if $\mathbf{f(u) \leq_B f(v).}$

Since **f** is injective it follows that one has an analog of the property in the last sentence for strict inequality**:**

For all $\mathbf{u, v \in A}$ *we have* $\mathbf{u <_A v}$ *if and only if* $\mathbf{f(u) <_B f(v).}$

The bijection **f** is usually called an **order – isomorphism,** but sometimes one sees other names like **similarity** or **similarity mapping;** one important advantage of the terms **"order – isomorphic"** and **"order – isomorphism"** is that such usage is consistent with standard mathematical usage in most other contexts.

The next result says that the property **"A** and **B** have the same order type**"** satisfies the conditions for an equivalence relation.

Theorem 1. *Every partially ordered set is order – isomorphic to itself by the identity mapping. If there is an order – isomorphism from the partially ordered set* **B** *to the partially ordered set* **A,** *then there is also an order-isomorphism from* **B** *to* **A.** *Finally, if there are order – isomorphisms from* **A** *to* **B** *and likewise from* **B** *to* **C,** *then there is an order – isomorphism from* **A** *to* **C.**

Sketch of proof. For the first sentence, one checks that the identity is an order – isomorphism. For the second part, one checks that if $\mathbf{f : A \to B}$ is an order-isomorphism, then so is $\mathbf{f^{-1}: B \to A}$. For the third part, one checks that if $\mathbf{f : A \to B}$ and $\mathbf{g : B \to C}$ are order – isomorphisms, then so is the composite $\mathbf{g \circ f : A \to C}$. ■

Example 1. The real numbers are order – isomorphic to the positive real numbers by the map sending $\mathbf{x}$ to $\mathbf{e^x}$. The inverse order – isomorphism from the positive real numbers to the real numbers is given by the natural logarithm function.

Example 2. The real numbers are order – isomorphic to the open interval $\mathbf{(-1, 1)}$ by the map sending $\mathbf{x}$ to $\mathbf{x/(1+|x|)}$.

Example 3. The nonnegative real numbers are order-isomorphic to the half – open interval $\mathbf{[0, 1)}$ by the restriction of the map in the previous example.

Note that there can be many order – isomorphisms from a partially ordered set to itself that are not equal to the identity. For example, on the open interval $\mathbf{(0, 1)}$ one has the infinite family of distinct maps $\mathbf{f(x) = x^n}$ for all positive integers $\mathbf{n}$. Similarly, for the rational numbers one has the infinite family of distinct order – isomorphisms expressible as $\mathbf{f(x) = cx}$, where $\mathbf{c}$ is an arbitrary positive rational number.

The conceptual meaning of order – isomorphism is that if the partially ordered sets $\mathbf{A}$ and $\mathbf{B}$ are order – isomorphic, then $\mathbf{A}$ has a given order – theoretic property if and only if $\mathbf{B}$ does. The following theorem gives several examples.

Theorem 2. *Let* $\mathbf{A}$ *and* $\mathbf{B}$ *be partially ordered sets which have the same order type, and let* $\mathbf{P}$ *be one of the properties listed below. Then* $\mathbf{A}$ *satisfies property* $\mathbf{P}$ *if and only if* $\mathbf{B}$ *does*:

- **(a)** *The partially ordered set is linearly ordered.*
- **(b)** *The partially ordered set is well – ordered.*
- **(c)** *The partially ordered set has a maximal element.*
- **(d)** *The partially ordered set has a minimal element.*
- **(e)** *The partially ordered set has a unique maximal element.*
- **(f)** *The partially ordered set has a unique minimal element.*
- **(g)** *Some element of the partially ordered set has an immediate predecessor.*
- **(h)** *Every element of the partially ordered set has an immediate predecessor.*
- **(i)** *The partially ordered set is finitely bounded from above.*
- **(j)** *The partially ordered set is finitely bounded from below.*
- **(k)** *The partially ordered set is a lattice.*

This list could be continued indefinitely. One additional example appears after the proof below.

Proof. We shall only do the first of these. The other cases follow the same pattern and the details are left to the reader as exercises.

Suppose that $\mathbf{A}$ and $\mathbf{B}$ have the same order type and let $\mathbf{f : A \to B}$ be an order – isomorphism. There are two cases depending upon whether $\mathbf{A}$ or $\mathbf{B}$ is already known to be linearly ordered. We shall begin with the first case.

We need to prove that the linear ordering property for **A** implies the linear ordering property for **B.** Let **x** and **y** be distinct elements of **B.** Since **f** is onto we may write **x = f(u)** and **y = f(v)** for some elements **u, v** in **A;** these must be distinct since they have different values under **f.** Therefore we either have **u < v** or **v < u.** If the first of these holds then since **f** is order preserving we have **x = f(u) < f(v) = y,** and if the second holds then we have the reversed expression **y = f(v) < f(u) = x.** Thus either **x < y** or **y < x,** which proves that **B** is also linearly ordered**.** This completes the proof in the first case**.**

On the other hand, if we know that **B** is linearly ordered, then we can prove **A** is linearly ordered using the preceding argument provided we switch the roles of **A** and **B** and replace **f** by its inverse (which is also an order – Isomorphism**;** verify this)**.**■

The preceding theorem is particularly useful for showing that two partially ordered sets do not have the same order type**.** Here is one more additional property that is particularly useful for showing that certain partially ordered sets do not have the same order type**.**

Definition. An ordered set **A** has the ***self – density property*** if

for each **x, y** *such that* **x < y** *there is some* **z** *such that* **x < z < y.**

Given two partially ordered sets **A** and **B** with the same order type**,** it follows as above that **A** *has the self – density property if and only if* **B** *does***.**■

Here are some additional examples**,** including some beyond those in Halmos and Lipschutz**:**

Examples. We claim that each of the linearly ordered sets $\mathbb{N}$**,** $\mathbb{Z}$ and $\mathbb{Q}$ of ***nonnegative integers***, ***(signed) integers***, and ***rational numbers*** is not order – isomorphic to any of the others in the list**.** The first one has a minimal element while the others do not**.** The third one has the self – density property displayed above while the others do not**.**

Example 4. The half-open intervals $[0, 1)$ and $(0, 1]$ are ***not*** order-isomorphic because one has a minimal element but no maximal element and the other has a maximal element but no minimal element**.**

Example 5. The half open interval $[0, 1)$ is isomorphic to $(0, 1]^{OP}$ (which is $(0, 1]$ with the **reverse** or **opposite** ordering)**,** and in fact the map sending **t** to **1 – t** is an explicit order – isomorphism**.**

Example 6. To complete the discussion of orderings on standard number systems, we claim that the set of real numbers $\mathbb{R}$ does not have the order type of $\mathbb{N}$**,** $\mathbb{Z}$ or $\mathbb{Q}$**.** For the first two of the latter**,** this is true because $\mathbb{R}$ has the self – density property while $\mathbb{N}$ and $\mathbb{Z}$ do not**.** Distinguishing $\mathbb{R}$ from $\mathbb{Q}$ requires a deeper understanding of the properties of the real number system**.** Specifically**,** one needs the boxed statement near the top of page 174 in Lipschutz**;** we shall discuss this distinguishing feature in the next unit of the notes**.**

V : Number systems and set theory

Any reasonable framework for mathematics should include the fundamental number systems which arise in the subject**:**

1. The ***natural numbers*** $\mathbb{N}$ (also known as the ***nonnegative integers***).
2. The (***signed***) ***integers*** $\mathbb{Z}$ obtained by adjoining negative numbers to $\mathbb{N}$**.**
3. The ***rational numbers*** $\mathbb{Q}$ obtained by adjoining reciprocals of nonzero integers to $\mathbb{Z}$**.**
4. The ***real numbers*** $\mathbb{R}$**,** which should include fundamental constructions like n^{th} roots of positive rational numbers for an arbitrary integer $n > 1$**,** and also all "infinite decimals" of the form $b_1 \cdot 10^{-1} + b_2 \cdot 10^{-2} + \ldots + b_k \cdot 10^{-k} + \ldots$ where each b_i belongs to $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$**.**

Up to this point we have tacitly assumed that such number systems are at our disposal**.** However**,** in both the naïve and axiomatic approaches to set theory it is eventually necessary to say more about them**.**

The naïve approach. In naïve set theory it is necessary to do two things**.** First**,** one must describe the properties that the set – theoretic versions of these number systems should satisfy**.** Second**,** something should be said to justify our describing such systems as **THE** natural numbers**,** **THE** integers**,** **THE** rational numbers**,** and **THE** real numbers**.** This usage suggests that we have completely unambiguous descriptions of the number systems in terms of their algebraic and other properties**.** One way of stating this is that

> ***any system satisfying all the conditions for one of the standard systems*** $\mathbb{N}$**,** $\mathbb{Z}$**,** $\mathbb{Q}$ ***or*** $\mathbb{R}$ ***should be the same as*** $\mathbb{N}$**,** $\mathbb{Z}$**,** $\mathbb{Q}$ ***or*** $\mathbb{R}$ ***for all mathematical purposes***,

with some explicit means for mechanical translation from the given system to the appropriate standard model**.** In less formal terms**,** it we have any systems **X** which satisfy all the fundamental properties of one of the systems $\mathbb{N}$**,** $\mathbb{Z}$**,** $\mathbb{Q}$ or $\mathbb{R}$**,** then **X** is essentially a ***mathematical clone*** of the appropriate number system**.**

There are good theoretical and philosophical reasons for asking such questions about the essential uniqueness of the number systems**,** but these question also have some important practical implications for the development of mathematics**.** If there would be two systems that satisfy the basic properties of $\mathbb{N}$**,** $\mathbb{Z}$**,** $\mathbb{Q}$ or $\mathbb{R}$ but differ from a standard model in some significant fashion**,** then clearly we might get different versions of mathematics depending upon which example is chosen**.** To illustrate this, suppose we decided to develop a version of the real numbers in which infinite base 10 "decimal expansions" are replaced by expansions with some other number base**,** say 16 (to conform with the internal arithmetic of some computer) or 60 (as in Babylonian mathematics)**.** We **expect** that everything should work the same regardless of the

numerical base we choose for expressing quantities, but at some point it is necessary to **confirm** that our expectation is fulfilled.

Later in this unit we shall describe precisely the notion of a mathematical clone. For the time being we note that examples of this concept have already been encountered in Section **IV.6** when we talked about whether two partially ordered sets have the same ***order type***. Given two such partially ordered sets, the $\mathbf{1-1}$ order preserving correspondence from one to another can be viewed as a formal mathematical way of saying that either of the partially ordered sets is a clone of the other.

Our coverage in this unit will mainly concern the first item described in the naïve approach; namely, the formal properties of the number systems and the mathematical statements of their uniqueness properties. Later in these notes (and largely for reference purposes) we shall explain why the basic properties describe these number systems in a totally unambiguous manner.

The axiomatic approach. In axiomatic set theory it is necessary to assume the existence of systems with the given properties and to prove these properties describe them unambiguously (the latter proceeds exactly the same as in naïve set theory).

One new issue in the axiomatic approach is the goal of keeping the basic assumptions for set theory as simple as possible. Assuming the existence of four separate but clearly interrelated number systems is a convenient first step, but at some point it is natural to ask if we really need to make such a long list of assumptions in order to set everything up. Aside from possible aesthetic considerations, there is the practical consideration that long lists of assumptions raise questions whether there might be some logical inconsistency; after all, the whole idea of a proof by contradiction is that one makes so many assumptions that the conclusions end up contradicting each other, and it would undermine everything if such contradictions could be derived from the axioms for set theory itself. We shall address some of these issues in the final units of the notes.

Some more specific objectives

Much of this unit is devoted to summarizing familiar properties of the four basic number systems, so we shall indicate some points that are less elementary and particularly important. In Section 1 the most significant new item is the statement of the Peano Axioms for the natural numbers, and in Section 2 the discussion of finite induction and recursive definitions in the framework of set theory is one of the main topics in the unit. The formulas for counting the numbers of elements in various finite sets in Section 3 start with familiar ideas, and they give systematic rules that are important both for their own sake and for the remaining units of the course. Finally, the description of the real numbers in Section 4 is fundamentally important. Although this description is fairly concise, it contains everything that is needed to justify the standard facts about real numbers and to develop calculus in a mathematically rigorous fashion. The latter development is covered in subsequent courses. Although the justification of the usual expansions for real numbers is also somewhat peripheral to the present course, for the sake of completeness we shall explain how our formal description of the real numbers yields their familiar properties which are used in everyday work, both inside and outside of mathematics.

V. 1 : The natural numbers and integers

(Halmos, §§ 11 – 13; Lipschutz, §§ 2.1, 2.7 – 2.9)

In many respects the positive integers form the most basic number system in all of the mathematical sciences. Some reasons for this are historical or philosophical, but logical considerations are particularly important for the systematic development of mathematics.

Clearly we would like our descriptions of number systems to summarize their basic algebraic properties concise but understandable. In particular, it simplifies things considerably if we can say that addition, subtraction and multiplication are always defined. Since the positive integers are not closed under subtraction, clearly they do not fulfill this condition. Therefore we shall begin by describing the integers, and we shall view the positive integers as a subset of the integers with certain special properties.

The important algebraic properties of the integers split naturally into three classes, two of which are fairly general and one of which is more focused.

Basic rules for addition and multiplication. Formally, these are the conditions defining an abstract type of mathematical system known as a ***commutative ring with unit.***

FIRST AXIOM GROUP FOR THE INTEGERS. *The integers are a set* $\mathbb{Z}$, *and they have binary operations* $\mathbf{A : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}}$, *normally expressed in the form* $\mathbf{A(u, v) = u + v}$, *and* $\mathbf{M : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}}$, *normally expressed in the form* $\mathbf{M(u, v) = uv}$ *or* $\mathbf{u \cdot v}$ *or* $\mathbf{u \times v}$, *which satisfy the following algebraic conditions:*

1. (Associative Laws). *For all* $\mathbf{a, b, c}$ *in* $\mathbb{Z}$, $\mathbf{(a + b) + c = a + (b + c)}$ *and* $\mathbf{(ab)c = a(bc)}$.
2. (Commutative Laws). *For all* $\mathbf{a, b}$ *in* $\mathbb{Z}$, $\mathbf{a + b = b + a}$ *and* $\mathbf{ab = ba}$.
3. (Distributive Law). *For all* $\mathbf{a, b, c}$ *in* $\mathbb{Z}$, $\mathbf{a(b + c) = ab + ac}$.
4. (Existence of 0 and 1). *There are distinct elements* $\mathbf{0, 1}$ *in* $\mathbb{Z}$ *such that for all* $\mathbf{a}$ *we have* $\mathbf{a + 0 = a}$, $\mathbf{a \times 0 = 0}$ *and* $\mathbf{a \times 1 = a}$.
5. (Existence of negatives or additive inverses). *For each* $\mathbf{a}$ *in* $\mathbb{Z}$ *there is an element* $\mathbf{-a}$ *in* $\mathbb{Z}$ *such that* $\mathbf{a + (-a) = 0}$.

Notational footnote: The notation $\mathbb{Z}$ for the integers has become fairly standard in mathematical writings, and it is apparently derived from the German word for numbers (*Zahlen*) and/or cyclic (*zyklisch*).

We shall need some consequences of the preceding algebraic conditions such as the following:

Proposition 0. *If* $\mathbf{a}$ *belongs to a system satisfying the properties listed above, then we have* $\mathbf{(-a)(-b) = ab}$. *In particular, when* $\mathbf{a = 1}$ *we have* $\mathbf{(-1)(-b) = b}$.

Proof. The following are special cases of the axioms**:**

$$0 = a0 = a[b + (-b)] = ab + a(-b)$$

$$0 = 0(-b) = [a + (-a)](-b) = a(-b) + (-a)(-b)$$

The preceding results also show that $ab = -[a(-b)] = (-a)(-b)$.■

Basic rules for ordering. When combined with the previous conditions**,** these yield a type of mathematical system known as an ***ordered integral domain.***

SECOND AXIOM GROUP FOR THE INTEGERS. *There is a linear ordering on* $\mathbb{Z}$ *such that the following hold***:**

1. *If* $a > 0$ *and* $b > 0$**,** *then* $a + b > 0$ *and* $ab > 0$**.**
2. *For all* a, b *in* $\mathbb{Z}$**,** *we have* $a > b$ *if and only if* $a - b > 0$**.**

Proposition 1. *If* **a** *and* **b** *belong to a system satisfying the arithmetic and ordering properties listed above, then* $a > b$ *if and only if* $-b > -a$**.**

Proof. We begin by showing that if a is nonzero then so is $-a$**.** This is true because $a + (-a) = 0$ and $(-a) = 0$ imply $a = a + 0 = 0$**.**

Next**,** we shall prove that $a > 0$ implies that $-a < 0$**.** If this were not the case**,** then the preceding paragraph implies that $-a > 0$**,** and it follows that $a + (-a) > 0$**;** since the left hand side is always zero**,** we have a contradiction**,** and therefore it follows that $-a < 0$**.**

Finally**,** if $a > b$ then $a - b > 0$**,** and this implies that

$$(-b) - (-a) = (-b) + (-(-a)) = (-b) + (-1)(-a) = (-b) + a = a - b > 0$$

which means that $(-b) > (-a)$**.** The converse statement follows directly from this and the fact that $x = 1 \cdot x = [(-1)(-1)] \cdot x = (-1)[(-1)x] = -(-x)$.■

Well – ordering of positive elements. This is the assumption that the set $\mathbb{N}$ of nonnegative elements in $\mathbb{Z}$**,** often called the ***natural numbers*****,** is well – ordered with respect to the standard linear ordering**.**

WELL - ORDERING AXIOM FOR THE NONNEGATIVE INTEGERS. *The set* $\mathbb{N}$ *of all* x *in* $\mathbb{Z}$ *such that* $x \geq 0$ *is well – ordered.*

We shall now derive some basic properties of the integers**.**

Lemma 2. *If* **x** *is a nonzero element in a system satisfying the first two groups of axioms, then* x^2 *is positive***.**

***Proof of Lemma* 2.** Either **x** is positive or $-x$ is positive**,** and in these respective cases it follows that x^2 is positive or $(-x)^2$ is positive. However**,** the previous proposition implies that $x^2 = (-x)^2$**,** and thus in either case we know that the square must be positive**.**■

Lemma 3. *The multiplicative identity* 1 *is positive, and there are no integers* **x** *for which we have* $0 < x < 1$.

***Proof of Lemma* 3.** First of all, 1 is positive because $1 = 1^2$. Let **P** be the set of positive elements in $\mathbb{Z}$. By well – ordering it follows that **P** has a least element **m,** which must satisfy $m \leq 1$. If strict inequality holds then we have $1 - m > 0$, and therefore we have $m(1 - m) > 0$, which translates to $0 < m^2 < m$, contradicting the minimality of **m.** Therefore **1** must be the least element of the positive integers.■

We shall need the following elementary but important property of positive integers later in this unit.

Theorem 4. (Long Division Theorem.) *Given two nonnegative integers* **a** *and* **b** such that $b > 1$, *there are* ***unique*** *nonnegative integers* **q** *and* **r** *such that* $a = bq + r$, *where* $0 \leq r \leq b - 1$.

The numbers **q** and **r** are often called the *integral quotient* and *remainder* respectively.

Proof. We first prove existence. Consider the set of all differences $a - bx$, such that **x** is a nonnegative integer and $a - bx$ is nonnegative. This set contains **a,** and thus it is nonempty, and as such it has a minimum element **y.** We claim that $y < b$; if this were false, then $y - x$ would be another element of the set (it is still nonnegative) and it would be strictly less than **y.** Since **y** is minimal this cannot happen, and therefore we must have $y < b$. This establishes existence.

To prove uniqueness, suppose that we have two expressions

$$a = bq + r = bq' + r',$$

where **q** and **q′** are nonnegative and (say) $0 \leq r \leq r' \leq b - 1$. These conditions imply that $0 \leq r' - r \leq b - 1$, and since

$$b(q' - q) = r' - r \leq b - 1$$

it follows that $b(q' - q) = 0$. Since **b** is positive this forces $q' - q$ to be equal to 0, so that $q' = q$. If we substitute this back into the first displayed equation in the paragraph we see that we must also have $r' = r$.■

The Peano Axioms for the natural numbers

There is a very simple and important characterization of $\mathbb{N}$ which is due to G. Peano (1858 – 1932). It depends upon two intuitively clear properties. The first is that zero is the unique nonnegative integer that is smaller than every other nonnegative integer, and the second is that if we are given a nonnegative integer **n,** then $n + 1$ is the unique minimal positive integer m such that $m > n$.

Definition. A ***system satisfying the Peano axioms*** is an ordered pair (P, σ) consisting of a set **P** and a function $\sigma: P \to P$ with the following properties [which reflect the nature of σ as a map taking each natural number **m** to its "successor" $m + 1$]:

(1) There is a distinguished element (the *zero element* **0** or $\mathbf{0_P}$) that is not in the image of σ.

(2) The map σ is $\mathbf{1-1}$.

(3) If **A** is a subset of **P** such that

(i) $0 \in A$,

(ii) for all $k \in P$, $k \in A$ implies $\sigma(k) \in A$,

then we must have $A = P$.

The third axiom is added to guarantee that **P** is the minimal set satisfying the axioms and containing **0.**

The next result should come as no surprise.

Theorem 5. *If* $\mathbb{N}$ *denotes the natural numbers and* $\sigma : \mathbb{N} \to \mathbb{N}$ *is the function defined by* $\sigma(m) = m + 1$, *then* (P, σ) *satisfies the Peano axioms.*

Proof, The first property follows because $\sigma(x) = 0$ implies $x = -1$, and hence **0** is not in the range of σ. The second follows because $\sigma(x) = \sigma(y)$ means that $x + 1 = y + 1$, and if we subtract **1** from each side we obtain $x = y$. To prove the third, suppose that **A** is not equal to $\mathbb{N}$. By well – ordering we know that $\mathbb{N} - A$ has a least element **m.** Since $0 \in A$, we know that $m > 0$. Furthermore, since **m** is the least element of $\mathbb{N} - A$ then it follows that $m - 1 \in A$. But now if we apply property **(ii)** we conclude that $m = \sigma(m - 1)$ must also lie in **A,** contradicting our assumption that **m** does not belong to **A.** The source of the contradiction is our assumption that **A** is a proper subset of $\mathbb{N}$, and hence this must be false, so that $A = \mathbb{N}$. ■

Uniqueness of the integers

At the beginning of this unit we indicated that our descriptions of number systems should essentially characterize them uniquely; in other words, we would like to say that if we are given two systems which satisfy our axioms for the integers, then they are the same for all mathematical purposes. This is analogous to the notion of order – isomorphism in Section **IV.6,** and the term ***isomorphism*** is also used to describe the sorts of mathematical equivalences that we shall consider here.

As in the case of partially ordered sets, we shall try to motivate the appropriate concept of isomorphism with an example: If we are given one system which satisfies the given list of properties for the integers, then it is possible to construct a second system by brute force as follows. Let $\mathbb{Z}$ be the original set with operations and order given in the usual manner. Then we can make the set $\mathbb{Z} \times \{0\}$ into a system satisfying the same properties by defining addition by the formula $(x, 0) + (y, 0) = (x + y, 0)$, multiplication by the formula $(x, 0) \cdot (y, 0) = (xy, 0)$, and ordering by the formula $(x, 0) < (y, 0)$ if and only if $x < y$. This may, and in fact ***should***, seem somewhat artificial, for there is an obvious $1 - 1$ correspondence **h** from $\mathbb{Z}$ to $\mathbb{Z} \times \{0\}$ such that $h(x + y) = h(x) + h(y)$,

h(x · y) = h(x) · h(y), and **h(x) < h(y)** if and only if **x < y.** In other words, the **1 – 1** correspondence **h** preserves all the basic structure. A map of this sort is known as an ***isomorphism***. The basic uniqueness result states that any two systems satisfying the listed properties for the integers are related by an isomorphism. Here is the formal statement.

Theorem 6. *Suppose that* **X** *and* **Y** *are sets with notions of addition, multiplication and ordering which satisfy all the conditions for the integers. Then there is a* ***unique*** **1 – 1** *correspondence from* **h** *from* **X** *to* **Y** *that is an* ***isomorphism*** *in the appropriate sense*:

> *For all elements* **u, v ∈ X** *we have* **h(u + v) = h(u) + h(v), h(u · v) = h(u) · h(v),** *and* **h(u) < h(v)** *if and only if* **u < v.** *The map* **h** *sends the zero and unit of* **X** *to the zero and unit of* **Y** *respectively*.

The existence of an isomorphism implies that any reasonable mathematical statement about the addition, multiplication and linear ordering of **X** is also true about **Y** and conversely. A proof of Theorem 6 appears in Unit **VIII.** The proof itself is relatively straightforward and elementary but somewhat tedious; however, it is absolutely necessary to establish such a result if we want to talk about **THE** integers.

V . 2 : Finite induction and recursion

(Halmos, §§ 11 – 13; Lipschutz, §§ 1.11, 4.6, 11.1 – 11.7)

Proofs by ***mathematical induction***, or more precisely by ***finite induction***, play an important role in the mathematical sciences and many of their applications to other subjects. Furthermore, as noted on page 48 of Halmos,

> *induction is often used not only to prove things but also to define things*

and because of this we shall describe both the proof definition processes explicitly in this section. Objects defined by induction are often said to be defined ***recursively*** (or by ***finite recursion***). Examples of recursive definitions arise throughout the mathematical sciences, including set theory itself, and therefore we shall describe the procedure fairly explicitly.

Description of the method

Mathematical induction is often a very powerful technique, but it is really more of a method to provide a formal verification of something that is suspected to be true rather than a tool for making intuitive discoveries, but it is absolutely essential. The use of mathematical induction dates back at least to some work of F. Maurolico (1494 – 1575). There are many situations in discrete mathematics where this method is absolutely essential.

Most of the remaining material on mathematical induction is adapted from the following online references:

http://www.cut-the-knot.org/induction.shtml

http://en.wikipedia.org/wiki/Mathematical_induction

IMPORTANT: The similarity between the phrases "mathematical induction" and "inductive reasoning" may suggest that the first concept is a form of the second, but ***this is not the case. Inductive reasoning is different from deductive reasoning***, while

mathematical induction is actually a form of deductive reasoning.

Proofs by mathematical induction involve a sequence of statements, one for each nonnegative integer **n** (sometimes it is impractical to start with **n = 0**, and one can begin instead with an arbitrary integer $\mathbf{n_0}$), and it is convenient to let **P(n)** denote the $\mathbf{n^{th}}$ statement. In the original example from the 16th century, **P(n)** was the familiar formula for the sum of the first **n** odd positive integers:

$$\mathbf{1 + 3 + 5 + \ldots + (2n - 1) = n^2}$$

In this case the first statement **P(1)** is $\mathbf{1 = 1^2}$, the statement **P(2)** is $\mathbf{1 + 3 = 2^2}$, the statement **P(3)** is $\mathbf{1 + 3 + 5 = 3^2}$, and so on.

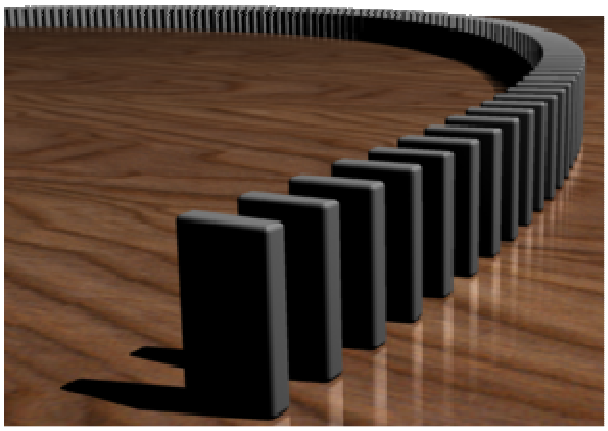
The method of proof by mathematical induction has two basic steps:

1. Proving that the first statement $\mathbf{P(n_0)}$ is true.
2. Proving that if **P(k)** is true for some value of **k**, then so is the next statement **P(k + 1)**.

In effect, *mathematical induction allows one to prove an* ***infinite list of statements***, say **P(1), P(2), P(3), ... ,** *with an argument that has only* ***finitely many steps.*** It may be helpful to visualize this in terms of the domino effect; if you have a long row of dominoes standing on end, you can be sure of two things:

1. The first domino can be pushed over.
2. Whenever a domino falls, then its next neighbor will also fall.

Under these conditions, we know that ***every one of the dominos in the picture below will eventually fall*** if the first one is nudged down in the right direction.



Here is a **YOUTUBE** video illustrating the domino effect**:**

http://www.youtube.com/watch?v=IV68b0JIG9k&feature=related

There are some instances where one uses a variant of the principle of mathematical induction stated above; namely, one replaces the assumption in the second step with a stronger hypothesis that **P(m)** is true for ***all*** **m < k + 1** and not just for **m = k.**

Example of a proof by induction. Here is a proof of the summation formula for the first **n** odd integers**.** The statement **P(1)** merely asserts that **1 = 1^2,** and hence it is obviously true**.** Let's assume we know that **P(k)** is also true for some arbitrary **k,** so that we have the equation **1 + 3 + 5 + ... + (2k – 1) = k^2.** The next step in mathematical induction is to derive **P(k+1)** from **P(k).** To do this**,** we note that

$$\begin{aligned} 1 + 3 + \ldots + (2k-1) + (2k+1) &= [1 + 3 + \ldots + (2k-1)] + (2k+1) \\ &= k^2 + (2k+1) \\ &= (k+1)^2 \end{aligned}$$

which shows that **P(k+1)** is also true because **2k + 1 = 2(k + 1) – 1.** Therefore the statement **P(n)** is true for all **n** and we have proven the general formula by mathematical induction**.**■

Formally**,** the difference between mathematical induction and inductive reasoning sis that the latter would check the first few statements, say **P(1), P(2), P(3), P(4),** and then conclude that **P(n)** holds for all **n.** *The inductive step* "**P(k)** implies **P(k+1)**" *is missing***.** Needless to say**,** inductive reasoning does not constitute a proof in the strict sense of deductive logic**.**

Frequently the verification of the first statement in a proof by induction is fairly easy or even trivial, but ***it is absolutely essential to include an explicit statement about the truth of the initial case,*** and also ***it is important to be sure that the inductive step works for every statement in the sequence.*** If these are not done**,** the final conclusion may be false and in some cases downright absurd**.**

Example. (Somewhat more difficult than the others) Consider the following defective "proof" that *a nonempty finite set (purportedly!) contains as many elements as one of its proper subsets*. This is vacuously true for the empty set, so assume it is true for a set with **k** elements. Let **S** be a set with **k + 1** elements**;** we need to show that some proper subset **T** contains the same number of elements as **S.** Let **T** be obtained from **S** by removing one element, and let **U** be obtained from **T** by removing one element. By the induction assumption we know that **#(T) = #(U),** and since we also know that **#(S) = #(T) + 1** and **#(T) = #(U) + 1** we conclude that **#(S) = #(T).** This is a ridiculous conclusion, so the point here is to ask**,** "*How did this happen?*" In fact**,** ***the inductive step we have given is valid for all values of* k *except for the case* k = 0.** However**,** when **k = 0** it breaks down because **T** must be the empty set, so it is not possible to construct the subset **U** by removing an element from **T.**

Justification of the method

In fact**,** there are two versions of proof by induction that are used frequently in the mathematical sciences**.** We shall state and prove both of them**.**

Theorem 1. (WEAK PRINCIPLE OF FINITE INDUCTION**.)** *Suppose that for each nonnegative integer* **n** *we are given a statement* **(S_n)** *such that the statements* **(S_n)** *satisfy the following conditions***:**

(i) **(S_0)** *is true***.**

(ii) *For all positive integers* **n,** *if* **(S_{n-1})** *is true***,** *then* **(S_n)** *is true***.**

Then *each of the statements* **(S_n)** *is true***.**

Proof: Let **F** be the set of all **n** such that **(S_n)** is false**.** We claim that **F** is empty; we shall assume the contrary and derive a contradiction**.**

If **F** is nonempty, then there is a least **m** such that **(S_m)** is false**,** and by the first assumption we know that **m** is positive, so that **m – 1** is nonnegative**.** By the minimal nature of **m** we know that **(S_{m-1})** must be true**.** Therefore the second condition implies that **(S_m)** is true**,** yielding a contradiction**.** The contradiction arises from our assumption that **F** is nonempty**,** and therefore the latter set must be empty**,** which means that each of the statements **(S_n)** is true**.**■

Frequently one needs a version of finite induction with a stronger hypothesis**.**

Thereom 2. (STRONG PRINCIPLE OF FINITE INDUCTION**.)** *Suppose that for each nonnegative integer* **n** *we are given a statement* **(S_n)** *such that the statements* **(S_n)** *satisfy the following conditions***:**

(i) **(S_0)** *is true***.**

(ii) *For all positive integers* **n,** *if* **(S_k)** *is true for all* **k < n,** *then* **(S_n)** *is true***.**

Then *each of the statements* **(S_n)** *is true***.**

Proof: Let **F** be the set of all **n** such that **(S_n)** is false**.** We claim that **F** is empty; we shall assume the contrary and derive a contradiction**.**

If **F** is nonempty, then there is a least **m** such that **(S_m)** is false**,** and by the first assumption we know that **m** is positive**,** so that the set of all **k** such that **k < m** is nonempty. By the minimal nature of **m,** we know **(S_k)** is true for all **k < m.** Therefore the second condition implies that **(S_m)** is true**,** yielding a contradiction**.** The contradiction arises from our assumption that **F** is nonempty**,** and therefore the latter set must be empty**,** which means that each of the statements **(S_n)** is true**.**■

One important example of a result whose proof requires the Strong rather than the Weak Principle of Finite Induction is the Fundamental Theorem of Arithmetic (see Rosen**,** Example 14**,** p. 250)**.** Another example illustrating the use of the Strong Principle of Finite Induction appears at the end of the next section**.**

Definition by recursion

The basic idea is fairly simple**.** We begin to define a function by specifying **f(0),** assume we know how to define **f(x)** for **x < n,** and we use this partial function to find **f(n).** Here is a formal statement of this principle**:**

Theorem 3. (Recursive Definition Theorem.) *Suppose that* $\mathbf{B}$ *is a set, and suppose also that for each nonnegative integer* $\mathbf{n}$ *we have a function* $\mathbf{H : B^{\{0, \ldots, n\}} \to B}$, *let* $\mathbb{N}$ *be the nonnegative integers, and let* $\mathbf{b_0 \in B}$. *Then there is a unique function* $\mathbf{f : \mathbb{N} \to B}$ *such that* $\mathbf{f(0) = b_0}$ *and for all positive* $\mathbf{n}$ *we have*

$$\mathbf{f(n) = H\big(f \,|\, \{0, \ldots, n-1\}\big).}$$

Proof. We begin by describing the approach to proving the result. The idea for proving existence is to define a sequence of functions $\mathbf{g_n : \{0, \ldots, n-1\} \to B}$ which agree on the overlapping subsets; one then constructs a function $\mathbf{f}$ whose graph is the union of the graphs of the partial functions. The uniqueness proof will then reduce to proving uniqueness for the restrictions to each subset $\mathbf{\{0, \ldots, n-1\}}$.

The function $\mathbf{g_0 : \{0\} \to B}$ is defined by $\mathbf{g_0(0) = b_0}$. Once we are given the function $\mathbf{g_n : \{0, \ldots, n-1\} \to B}$. we define the function $\mathbf{g_{n+1} : \{0, \ldots, n\} \to B}$ by $\mathbf{g_{n+1}(k) = g_n(k)}$ if $\mathbf{k < n}$ and $\mathbf{g_{n+1}(n) = H(g_n)}$. Let $\mathbf{G_n \subset \{0, \ldots, n-1\} \times B}$ be the graph of $\mathbf{g_n}$, and let $\mathbf{G \subset \mathbb{N} \times B}$ be the union of the subsets $\mathbf{G_n}$.

We claim that for each $\mathbf{x \in \mathbb{N}}$ there is a unique $\mathbf{y \in B}$ such that $\mathbf{(x, y) \in G}$. If true, then this will imply the existence of a function $\mathbf{f : \mathbb{N} \to B}$ whose graph is equal to $\mathbf{G}$. Since $\mathbf{G}$ is the union of the graphs $\mathbf{G_n}$, this is equivalent to verifying that for all $\mathbf{n > x}$ the elements $\mathbf{g_n(x)}$ are all equal; note that $\mathbf{g_n(x)}$ is only defined for these values of $\mathbf{n}$. We shall prove that $\mathbf{g_{x+m}(x) = g_{x+1}(x)}$ for all $\mathbf{m > 1}$ by induction on $\mathbf{m}$; by construction we know that $\mathbf{g_n(x) = g_{n+1}(x)}$ for $\mathbf{n}$ as above. Therefore if $\mathbf{m = 2}$ we know that $\mathbf{g_{x+2}(x) = g_{x+1}(x)}$, yielding the first step of the inductive proof. If we know the result for $\mathbf{m}$, we can obtain it for $\mathbf{m + 1}$ by once again applying the identity $\mathbf{g_n(x) = g_{n+1}(x)}$. This proves that $\mathbf{G}$ satisfies the required property for the graph of a function from $\mathbb{N}$ to $\mathbf{B}$.

Finally, we need to prove uniqueness. Suppose that $\mathbf{f'}$ is an arbitrary function satisfying the given properties, and let $\mathbf{f}$ be constructed as in the previous paragraphs. We shall prove that the restrictions of $\mathbf{f}$ and $\mathbf{f'}$ to each subset $\mathbf{\{0, \ldots, n-1\}}$ are equal by induction on $\mathbf{n}$. If $\mathbf{n = 1}$ then uniqueness follows because the assumptions imply that the values of both $\mathbf{f}$ and $\mathbf{f'}$ at $\mathbf{0}$ are equal to $\mathbf{b_0}$. Suppose now that the restrictions of $\mathbf{f}$ and $\mathbf{f'}$ to the subset $\mathbf{\{0, \ldots, n-1\}}$ are equal; to prove the inductive step, it will suffice to show that $\mathbf{f(n) = f'(n)}$. But this follows from the equalities

$$\mathbf{f(n) = H\big(f \,|\, \{0, \ldots, n-1\}\big) = H\big(f' \,|\, \{0, \ldots, n-1\}\big) = f'(n),}$$

where the first equation is true by construction, the second is true by the induction hypothesis, and the third is true by the assumption on $\mathbf{f'}$.■

Typical recursive definitions

In practice, recursive definitions are usually stated in a less formal manner than indicated by the existence and uniqueness result. Probably the best way to illustrate this is to give simple examples as one would see it in a semi – formal mathematical

discussion and to analyze it in terms of the formal statement of the Recursive Definition Theorem. We begin with one which arises in numerous contexts.

Solutions to difference equations. Suppose that we are given a sequence of objects (say numbers, vectors, matrices or functions) **a(n)** in a set **A** which has a reasonable notion of addition. We would like to create a new sequence **b(n)** such that for each **n** the difference between consecutive terms **b(n + 1) – b(n)** is equal to **a(n).** Such an equation is often called a *first order difference equation*, and in some respects the theory of solutions to difference equations resembles the theory of solutions to differential equations. In particular, solutions to first order equations generally exist if one properly specifies an ***initial value*** **b(0)** for the sequence. It should be clear that we can uniquely define **b(n)** by the conditions given here, but we would also like to explain how this fits into the framework of the Recursive Definition Theorem. According to that result, for each **n** we need to define a suitable function $\mathbf{H : A^{\{0, \ldots, n\}} \to A}$, and one simple way of doing so is to take **H(g) = g(n) + a(n).** The conditions of the Recursive Definition Theorem then imply that one obtains a unique function **b(n)** satisfying the given conditions.■

Here is a more abstract type of example within set theory itself.

Proposition 4. *Let* **A** *be an infinite subset of the nonnegative integers* $\mathbb{N}$. *Then there is a strictly order – preserving* **1 – 1** *mapping* **f** *from* $\mathbb{N}$ *to* **A.**

Proof. **(***)** Define the function **f** recursively as follows: Take **f(0)** to be the least element of **A.** Suppose that we have a **1 – 1** strictly order – preserving mapping **f** defined from the finite set **{0, … , n – 1}** to **A.** Since **A** is infinite it follows that the image **f [{0, … , n – 1}]** is a proper subset of **A**, so that its complement is nonempty and there is some element of **A** which is greater than every element in **f [{0, … , n – 1}].** Now take **f(n)** to be the least such element of **A.** We claim the latter recursively defines **f;** this will be discussed further in the next paragraph. To complete the recursive step in the argument, we need to show that the newly extended function **f** on **{0, … , n}** is also strictly order – preserving. This follows because **f** is already known is strictly order – preserving on **{0, … , n – 1}** and by construction **f(n) > f(j)** for all **j < n.**■

We now need to analyze the construction of **f** and see how it can be formalized to fulfill all the conditions in the Recursive Definition Theorem. The main thing that does not appear in our discussion is a ***complete and explicit*** means for defining an element of **A** given an arbitrary mapping from **{0, … , n – 1}** to **A.** In our recursive definition we assumed that the function defined on the finite piece of $\mathbb{N}$ was strictly increasing, and at each step we showed that the extended function was also strictly increasing. Strictly speaking, we need to define an element of **A** even for partial functions that are not strictly increasing, but the precise nature of these definitions is unimportant because we shall never need the definitions for functions that are not strictly increasing. Formally, *one can define the function for such irrelevant sequences by some simple arbitrary device*. For example, in our setting we can simply take the value for one of the "irrelevant" partial functions to be the unique least element of **A.** If there are ever circumstances in which it is not clear how to define a value for "irrelevant" partial functions, one standard way is to work inside the slightly larger set $\mathbf{A \cup \{A\}}$ (recall this properly contains **A**) and simply define the value at the irrelevant functions to be the extra element **A.**■

V . 3 : Finite sets

(Halmos, §§ 11 – 13; Lipschutz, §§ 1.8, 3.2)

Courses in discrete structures and combinatorics study questions about finite sets extensively**.** In this section we shall develop a few basic aspects of this topic that will be needed or useful later in the course**.**

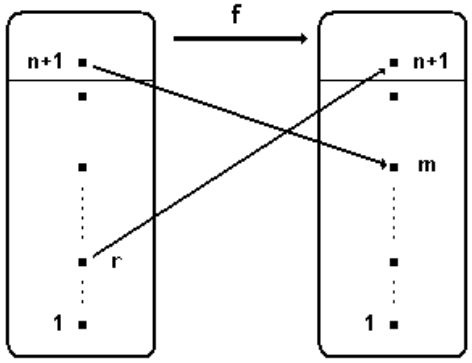
For our purposes a set **X** will be said to be ***finite*** if *there is some positive integer* **n** *for which there is a* ***1 – 1*** *correspondence from* **X** *to* **{1, … , n }.**

The pigeonhole principle

Experience indicates that if **X** is a finite set**,** then there is no **1 – 1** correspondence between **X** and a proper subset of itself**.** Our first objective is to give a rigorous proof of this basic fact**.**

Theorem 1. *Suppose that* **A** *is a finite set,* **B** *is a subset of* **A,** *and* $\mathbf{f: A \to A}$ *is a* $\mathbf{1-1}$ *mapping with* $\mathbf{f[A] = B}$**.** *Then* $\mathbf{B = A}$**.**

Proof. **(**)** We shall first consider the special case where $\mathbf{A = \{1, 2, \dots, n\}}$ and proceed by induction on **n.** If $\mathbf{n = 1}$ then the result is trivial. Suppose it is true for **n** and proceed to the case of $\mathbf{n + 1}$**.** Call this set **A,** and let **C** be the set of the first **n** elements**.** If $\mathbf{f[C]}$ is contained in **C** then by induction $\mathbf{f[C] = C}$ and we must then have $\mathbf{f(n + 1) = n + 1}$**.** Suppose now that $\mathbf{f[C]}$ is not contained in **C.** Since **f** is $\mathbf{1-1}$**,** it follows that $\mathbf{f(n + 1)}$ cannot be equal to $\mathbf{n + 1}$**,** and therefore we must have $\mathbf{f(r) = n + 1}$ for some $\mathbf{r < n + 1}$ and also $\mathbf{f(n + 1) = m < n + 1}$**.** Define a new function $\mathbf{g : C \to C}$ by setting $\mathbf{g(r) = m}$ and $\mathbf{g(k) = f(k)}$ otherwise**.**

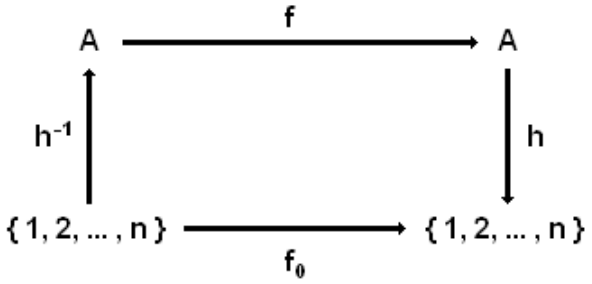


CLAIM: **g** is a **1 – 1** mapping**.** Suppose that $\mathbf{g(i) = g(j)}$**.** Since $\mathbf{f = g}$ for $\mathbf{x \neq r}$ it follows that one of **i** and **j** must be equal to **r,** so say $\mathbf{j = r}$**.** Then $\mathbf{g(i) = f(i)}$ and also $\mathbf{g(r) = m = f(n + 1)}$**.** Since $\mathbf{i < n + 1}$ and **f** is $\mathbf{1-1}$**,** it follows that $\mathbf{g(i) \neq}$

$g(r)$ and consequently g is a $1-1$ mapping. By induction g, which is defined on the set $\{1, 2, \dots, n-1\}$, is also onto.

We shall use the preceding paragraph to prove that f is also onto. If $y < n+1$, then $y = g(z)$ for some $z \in C$, and since $g(z) = f(w)$ for some w, it follows that the image of f contains all of C. Since we have shown that $n+1 = f(r)$ it follows that the image of f contains all of A, provided that $A = \{1, 2, \dots, n\}$.

To prove the general case, let A be a finite set with n elements, so that there is a $1-1$ onto mapping h from A to $\{1, 2, \dots, n\}$. Given a $1-1$ mapping $f : A \to A$, let f_0 be the conjugate mapping from $\{1, 2, \dots, n\}$ to itself defined by $f_0 = hfh^{-1}$.



We claim that f_0 is a $1-1$ mapping. Suppose that $f_0(x) = f_0(y)$; by definition of f_0 we have $hfh^{-1}(x) = hfh^{-1}(y)$. Since the mappings h, f and h^{-1} are all $1-1$ we can successively use the injectivity of h to conclude that that $fh^{-1}(x) = fh^{-1}(y)$, the injectivity of f to conclude that that $h^{-1}(x) = h^{-1}(y)$, and the injectivity of h^{-1} to conclude that that $x = y$. Therefore f_0 is $1-1$, and therefore the preceding argument shows that f_0 is also onto.

To prove that f is onto, suppose that $z \in A$, and let $w = h(z)$. By the special case established above, it follows that $w = f_0(v)$ for some v, so that

$$z = h^{-1}(w) = h^{-1}(f_0(v)) = h^{-1}(hfh^{-1}(v)) = fh^{-1}(v)$$

which implies that f must be onto.■

Counting elements of finite sets

If X is a finite set, there is a unique natural number n such that there is a $1-1$ correspondence between X and $\{1, \dots, n\}$; uniqueness follows from the previous discussion in this section. Following standard practice we say that X *has* n *elements* if this is the case, and we write $|X| = n$.

Our first result looks obvious, but we still need to prove it.

Proposition 2. ***If*** B *is a subset of* A, *then* $|B| \leq |A|$.

Proof. We proceed by induction on $n = |A|$. If $n = 0$ then the result is trivial because A is empty and hence B is also empty, so we have $|B| = 0 \leq 0 = |A|$. Suppose the result is known for $|A| = k$, and consider the case where $|A| = k+1$.

Let $f : \{1, \ldots, k+1\} \to A$ be a $1-1$ correspondence, and let B be a subset of A. Let C be the subset of A obtained by removing $f(k+1)$, and let D denote the intersection of B and C. By construction $|C| = k$ and D is a subset of C, and therefore by the induction hypotheses we have $|D| \leq k$. There are now two cases depending upon whether or not $f(k+1)$ belongs to B. If so, then $D = B$ and hence $|B| = |D| \leq k < |A|$. If not, then $B = D \cup \{f(k+1)\}$ and hence $|B| = |D| + 1 \leq k+1 = |A|$. This completes the proof of the inductive step. ■

Corollary 3. *If* B *is a* ***proper*** *subset of* A, *then* $|B| < |A|$.

This follows immediately by combining the previous two results. ■

The following basic formulas for counting elements of finite sets have important counterparts for infinite sets that will be discussed in Unit V.

Theorem 4. *Let* A *and* B *be sets with* n *and* m *elements respectively.*

1. *If* A *and* B *are disjoint, then* $|A \cup B| = n + m$.
2. *For arbitrary finite sets* A *and* B *we have* $|A \times B| = n \cdot m$.
3. *If* A *and* B *are arbitrary finite sets and* B^A *is the set of functions from* A *to* B, *then we have* $|B^A| = m^n$.

Proof. All of the proofs proceed by induction on $n = |A|$.

Verification of **(1):** If $n = 0$ then $A \cup B = B$ and therefore $m = |B| = |A \cup B| = 0 + m$. Suppose the result is true for $n = k$, suppose also that $|A| = k+1$, suppose we have a $1-1$ correspondence between A and $\{1, \ldots, k+1\}$, let $C \subset A$ correspond to $\{1, \ldots, k\}$, and let z be the unique element of A such that $A = C \cup \{z\}$. By induction there is a $1-1$ correspondence $g : \{1, \ldots, k+m\} \to C \cup B$. Define a new function $f : \{1, \ldots, k+m+1\} \to A \cup B$ such that $f = g$ on $\{1, \ldots, k+m\}$ and $f(k+m+1) = z$.

We claim that f is $1-1$ and onto. Suppose that $f(x) = f(y)$. If neither x nor y is equal to $k+m+1$, then $g(x) = f(x)$ and $g(y) = f(y)$, and since g is $1-1$ it follows that $x = y$. Suppose now that, say, $x = k+m+1$. Then $f(x) = z$. On the other hand, if $f(y) = z$ then the only possibility is $k+m+1$, and hence $x = y$ in this case too. Therefore f is a $1-1$ mapping. Suppose now that w belongs to $A \cup B$; we need to show that w lies in the image of f. If w is not equal to z then we have $w = g(j)$ for some $j < k+m+1$, and thus we also have $w = f(j)$ for the same choice of j. On the other hand, if $w = z$ then we have $z = f(k+m+1)$. Therefore f is $1-1$ and onto, so this completes the proof of the inductive step.

Verification of **(2):** If $n = 0$ then $A \times B = \emptyset$ and therefore $0 = |\emptyset| = |\emptyset \times B| = 0 \cdot m$. Suppose once again the result is known to be true for $n = k$, and suppose also that $|A| = k+1$ with some given $1-1$ correspondence from A to $\{1, \ldots, k+1\}$. Let $C \subset A$ correspond to $\{1, \ldots, k\}$, and let z be the unique element of A such that $A = C \cup \{z\}$. By the induction hypothesis there is a $1-1$ correspondence $g : \{1, \ldots, k \cdot m\}$

$\rightarrow$ **C** $\times$ **B.** Let **h**:{**1, … , m**} $\rightarrow$ **B** be a $1-1$ correspondence, and define a new function **f**:{**1, … , k**$\cdot$(**m** + **1**)} $\rightarrow$ **A** $\times$ **B** such that **f** = **g** on {**1, … , k**$\cdot$**m**} and

$$\mathbf{f}(\mathbf{k}\cdot\mathbf{m} + \mathbf{j}) = (\mathbf{z}, \mathbf{h}(\mathbf{j}))$$

for **j** = **1, … , m.**

We claim that **f** is $1-1$ and onto. Suppose that **f**(**x**) = **f**(**y**). If neither **x** nor **y** greater than **k**$\cdot$**m**, then **g**(**x**) = **f**(**x**) and **g**(**y**) = **f**(**y**), and since **g** is $1-1$ it follows that **x** = **y.** Suppose now that, say, we have **x** > **k**$\cdot$**m.** Then **f**(**x**) = (**z, b**) for some **b** in **B**, and hence **f**(**y**) = (**z, b**). By construction, the only way this can happen is if **y** is also greater than **k**$\cdot$**m.** Therefore we may write **x** = **k**$\cdot$**m** + **i** and **y** = **k**$\cdot$**m** + **j** for some integers **i** and **j** between **1** and **m.** Since **f**(**x**) = **f**(**y**), it follows from the construction that **h**(**i**) = **h**(**j**) = **b**, and the latter in turn implies that **i** = **j.** Therefore we have **x** = **y** and hence **f** is $1-1$. Suppose now that **w** belongs to **A** $\times$ **B**; we need to show that **w** lies in the image of **f.** If the first coordinate of **w** is not equal to **z** then in fact we have **w** = **g**(**j**) for some **j** $\leq$ **k**$\cdot$**m**, and thus we also have **w** = **f**(**j**) for the same choice of **j.** On the other hand, if the first coordinate of **w** is equal to **z**, then write **w** = (**z, b**). By construction **b** = **h**(**j**) for some **j**, and it then follows that **w** = (**z, b**) = **f**(**k**$\cdot$**m** + **j**). Therefore **f** is $1-1$ and onto, so this completes the proof of the inductive step.

Verification of **(3): (***)** If **n** = **0** then there is a unique function from **A** = **Ø** to **B**; namely, the function whose graph is the empty set. Therefore we have $|\mathbf{B}^{\mathbf{A}}| = |\mathbf{B}^{\emptyset}| = \mathbf{1} = \mathbf{m}^{\mathbf{0}}$. Suppose again the result is known to be true for **n** = **k**, suppose also |**A**| = **k** + **1**, and assume we have a $1-1$ correspondence between **A** and {**1, … , k** + **1** }. Let **C** $\subset$ **A** correspond to {**1, … , k**}, and as before let **z** be the element of **A** such that **A** = **C** $\cup$ {**z**}. By induction there is a $1-1$ correspondence **g**:{**1, … ,** $\mathbf{m}^{\mathbf{k}}$} $\rightarrow$ $\mathbf{B}^{\mathbf{C}}$.

By the result in the preceding part of the theorem, it will suffice to construct a $1-1$ correspondence between $\mathbf{B}^{\mathbf{A}}$ and $\mathbf{B}^{\mathbf{C}} \times \mathbf{A}$, for then one obtains the equations

$$|\mathbf{B}^{\mathbf{A}}| = |\mathbf{B}^{\mathbf{C}} \times \mathbf{A}| = \mathbf{m}^{\mathbf{k}}\cdot\mathbf{m} = \mathbf{m}^{\mathbf{k+1}}$$

which is what we need to prove in order to verify the inductive step. Suppose now that we are given a function **u** : **A** $\rightarrow$ **B.** Consider the mapping Ω: $\mathbf{B}^{\mathbf{A}} \rightarrow \mathbf{B}^{\mathbf{C}} \times \mathbf{A}$ defined by Ω (**u**) = (**u**|**C**, **u**(**z**)); we claim that Ω is **1** – **1** and onto.

Suppose first that Ω (**u**) = Ω (**v**). Then by construction we have **u**|**C** = **v**|**C** and **u**(**z**) = **v**(**z**). Combining these with **A** = **C** $\cup$ {**z**}, we see that **u**(**t**) = **v**(**t**) for all **t** $\in$ **A**, and therefore we must have **u** = **v.** Therefore Ω is $1-1$. Suppose now that we are given an arbitrary pair (**g, b**). Then there exists a function **f** such that **f**(**t**) = **g**(**t**) for all **t** $\in$ **C** and **f**(**z**) = **b**, and therefore Ω is onto as required.■

Note. The result in the third part of the theorem illustrates one important reason for using $\mathbf{B}^{\mathbf{A}}$ to denote the set of all functions from **A** to **B.**

Boolean algebras of subsets

We shall prove a result relating the properties of finite sets to the Strong Principle of Finite Induction that was formulated in the preceding section.

Definition. Given a set **A,** let **P(A)** be the set of all subsets with the algebraic operations of union, intersection, and relative complementation. A ***Boolean subalgebra*** of **P(A)** is a subset $\mathbf{S} \subset \mathbf{P(A)}$ such that **S** is contained in **P(A),** it contains **A** and the empty set, it is closed under taking finite unions and intersections, and it is also closed under taking relative complements**.**

The simplest examples of Boolean subalgebras are given by equivalence relations**.** Specifically**,** if ***R*** is an equivalence relation on **A** and **S** is the family of all subsets that are unions of ***R –*** equivalence classes**,** then it is a routine exercise to verify that **S** is a Boolean subalgebra of **P(A).** The result below shows that all Boolean subalgebras have this form if **A** is a finite set**.**

Proposition 5. *Let* **A** *be a set, and let* **S** *be a Boolean subalgebra of* **P(A).** *Then there is an equivalence relation such that the subsets of* **S** *are the unions of* ***R –*** *equivalence classes.*

Proof. **(**)** A subset $\mathbf{Y} \in \mathbf{S}$ is said to be *atomic* for **S** if it is nonempty and there are no nonempty subsets $\mathbf{X} \in \mathbf{S}$ that are properly contained in **Y.** We shall prove the proposition by verifying the following two assertions**:**

1. Every subset of **S** is a union of atomic subsets.
2. Two atomic subsets of **S** are either disjoint or identical.

By previous results**,** it will follow that the atomic subsets are the equivalence classes for some equivalence relation on **A.**

We shall prove the first statement by induction on $|\mathbf{A}|$**.** If **A** has **0** or **1** element**,** then **S** must be equal to **P(A),** and for any finite set **A** a subset is atomic for **P(A)** if and only if it contains exactly one element**.** Suppose now that the result is true for all sets **B** such that $|\mathbf{B}| < |\mathbf{A}|$**.** There are two cases depending upon whether **S** contains a nonempty proper subset**.** If it does not**,** then **S** only consists of **A** and the empty set**,** and therefore **A** must be atomic**.** On the other hand, if **S** contains a nonempty proper subset **C,** then it also contains $\mathbf{A} - \mathbf{C} = \mathbf{D}$**,** and **D** is also a nonempty proper subset**.** It follows that both $|\mathbf{C}|$ and $|\mathbf{D}|$ are strictly less than $|\mathbf{A}|$**.**

Let $\mathbf{S}|\mathbf{C}$ and $\mathbf{S}|\mathbf{D}$ denote the set of all subsets in **S** that are contained in **C** and **D** respectively**.** We claim that these are Boolean subalgebras of **P(C)** and **P(D)** respectively**;** by our hypotheses we know that the empty set lies in both, that **C** and **D** are contained in $\mathbf{S}|\mathbf{C}$ and $\mathbf{S}|\mathbf{D}$ respectively**,** and that both of the latter are closed under finite unions or intersections (because the same is true for **S**)**.** To show these families are closed under relative complementation**,** note that if **X** lies in $\mathbf{S}|\mathbf{C}$ or then

$$\mathbf{C} - \mathbf{X} = \mathbf{C} \cap \mathbf{A} - \mathbf{X}$$

shows that **C – X** also belongs to **S|C,** and similar considerations show that if **X** lies in **S|D** then **D – X** also lies in **S|D.** By the induction hypothesis it follows **C** and **D** are unions of atomic subsets**,** and therefore the same is true for **A = C ∪ D.**

To complete the proof**,** we need to prove the second assertion given above; specifically, we need to prove that two atomic subsets are either disjoint or identical**.** But if **X** and **Y** are atomic subsets of **S,** then the Boolean subalgebra condition implies that **X ∩ Y** also belongs to **S.** Since it is contained in the minimal nonempty subsets **X** and **Y,** either the intersection is empty or else if it is nonempty then it must be equal to both **X** and **Y.**■

An abstract ***Boolean algebra*** is an algebraic system consisting of a set **A** together with three operations**;** namely**,** two binary operations **∪, ∩** and one unary operation (sending an element **x** to **x′**) which have the formal properties of unions, intersections, and complements**.** Chapter 11 of Lipschutz contains further material on such structures**,** with emphasis on computational techniques**.** An entirely different perspective on Boolean algebras**,** which reflects their role in modern pure mathematics**,** is contained in the following reference (which is written at the graduate level)**:**

> P. R. Halmos, ***Lectures on Boolean algebras*** (Originally published as Van Nostrand Math. Studies, No. 1). Springer – Verlag, New York, 1974. ISBN: 0 – 387 – 90094 – 2.

V . 4 : The real numbers

(Lipschutz, §§ 2.2 – 2.6, 7.7)

Following the approach of Section 1**,** we shall give an axiomatic description of the real numbers in terms of their basic properties. Many of these properties are also properties of the integers**,** but there are also some important new ones**.**

Basic rules for addition and multiplication. Formally, these are the conditions defining an abstract type of mathematical system known as a ***field.*** The first five of these are the previously introduced properties for a commutative ring with unit**,** and the final one reflects an important difference between the integers in the real numbers**;** in the latter one can divide by nonzero numbers**,** but usually this is not possible within the integers**.**

FIRST AXIOM GROUP FOR THE REAL NUMBERS. *The* **real numbers** *are a set* $\mathbb{R}$**,** *and they have binary operations* $\mathbf{A} : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ (addition)**,** *which is normally expressed in the form* $\mathbf{A(u, v) = u + v}$**,** *and* $\mathbf{M} : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ (multiplication)**,** *which is normally expressed in the form* $\mathbf{M(u, v) = u\,v}$ *or* $\mathbf{u \cdot v}$ *or* $\mathbf{u \times v}$**,** *such that the following algebraic conditions are satisfied***:**

1. (Associative Laws) *For all* $\mathbf{a, b, c}$ *in* $\mathbb{R}$, *we have* $(\mathbf{a} + \mathbf{b}) + \mathbf{c} = \mathbf{a} + (\mathbf{b} + \mathbf{c})$ *and* $(\mathbf{a}\,\mathbf{b})\,\mathbf{c} = \mathbf{a}\,(\mathbf{b}\,\mathbf{c})$.
2. (Commutative Laws) *For all* $\mathbf{a, b}$ *in* $\mathbb{R}$, *we have* $\mathbf{a} + \mathbf{b} = \mathbf{b} + \mathbf{a}$ *and* $\mathbf{a}\,\mathbf{b} = \mathbf{b}\,\mathbf{a}$.
3. (Distributive Law) *For all* $\mathbf{a, b, c}$ *in* $\mathbb{R}$, *we have* $\mathbf{a}\,(\mathbf{b} + \mathbf{c}) = \mathbf{a}\,\mathbf{b} + \mathbf{a}\,\mathbf{c}$.
4. (Existence of 0 and 1) *In* $\mathbb{R}$ *there are distinct elements* $\mathbf{0}, \mathbf{1}$ *such that for all* $\mathbf{a}$ *we have* $\mathbf{a} + \mathbf{0} = \mathbf{a}$, $\mathbf{a} \cdot \mathbf{0} = \mathbf{0}$ *and* $\mathbf{a} \cdot \mathbf{1} = \mathbf{a}$.
5. (Existence of negatives or additive inverses). *For each* $\mathbf{a}$ *in* $\mathbb{R}$ *there is an element* $-\mathbf{a}$ *in* $\mathbb{R}$ *such that* $\mathbf{a} + (-\mathbf{a}) = \mathbf{0}$.
6. (Existence of reciprocals or multiplicative inverses) *For each* $\mathbf{a} \neq \mathbf{0}$ *in* $\mathbb{R}$ *there is an element* $\mathbf{a}^{-1}$ *in* $\mathbb{R}$ *such that* $\mathbf{a} \cdot \mathbf{a}^{-1} = \mathbf{1}$.

Basic rules for ordering. These are the same as the ordering properties for the integers. When combined with the previous conditions, these yield a type of mathematical system known as an ***ordered field.***

SECOND AXIOM GROUP FOR THE REAL NUMBERS. *There is a linear ordering on* $\mathbf{R}$ *such that the following hold:*

1. *If* $\mathbf{a} > \mathbf{0}$ *and* $\mathbf{b} > \mathbf{0}$, *then* $\mathbf{a} + \mathbf{b} > \mathbf{0}$ *and* $\mathbf{a}\,\mathbf{b} > \mathbf{0}$.
2. *For all* $\mathbf{a, b}$ *in* $\mathbb{R}$, *we have* $\mathbf{a} > \mathbf{b}$ *if and only if* $\mathbf{a} - \mathbf{b} > \mathbf{0}$.

Basic rules for completeness of the ordering. The ordering on the real numbers satisfies an additional fundamental condition called the ***Dedekind completeness axiom*** after R. Dedekind (1831 – 1916), who formulated this property. In order to state this axiom it is necessary to introduce some additional standard definitions.

Definitions. Let $(\mathbf{L}, \leq)$ be a linearly ordered set, and let $\mathbf{A}$ be a subset of $\mathbf{L}$. An element $\mathbf{x} \in \mathbf{L}$ is said to be an *upper bound* for $\mathbf{A}$ in $\mathbf{L}$ if for each $\mathbf{a} \in \mathbf{A}$ we have $\mathbf{a} \leq \mathbf{x}$; note that the definition contains no information on whether $\mathbf{x}$ belongs to $\mathbf{L}$. An upper bound $\mathbf{x}$ is said to be a ***least*** *upper bound* (for $\mathbf{A}$ in $\mathbf{L}$) if for **every** upper bound $\mathbf{y}$ for $\mathbf{A}$ we have $\mathbf{x} \leq \mathbf{y}$.

Proposition 1. *If* $\mathbf{x}$ *and* $\mathbf{z}$ *are least upper bounds for a subset* $\mathbf{A}$ *as above, then* $\mathbf{x} = \mathbf{z}$.

Proof. Since $\mathbf{x}$ is a least upper bound and $\mathbf{z}$ is an upper bound, we have $\mathbf{x} \leq \mathbf{z}$. Similarly, since $\mathbf{x}$ is a least upper bound and $\mathbf{z}$ is an upper bound, we have $\mathbf{z} \leq \mathbf{x}$. Combining these, we conclude that $\mathbf{x} = \mathbf{z}$. ■

If a set $\mathbf{A}$ has a least upper bound $\mathbf{x}$, then we often write $\mathbf{x} = \text{L.U.B.}(\mathbf{A})$ or $\mathbf{x} = \mathbf{sup(A)}$. The symbolism **sup** is an abbreviation for the quasi – Latin term for the least upper bound; namely, the *supremum*.

There are dual notions for the reverse ordering on a linearly ordered set. Specifically, if $\mathbf{B}$ is a subset of $\mathbf{L}$ then a *lower bound* is a number $\mathbf{y}$ such that $\mathbf{y} \leq \mathbf{b}$ for all $\mathbf{b} \in \mathbf{B}$; note that the definition contains no information on whether $\mathbf{x}$ belongs to $\mathbf{L}$. A ***greatest*** *lower bound* is a lower bound $\mathbf{y}$ such that $\mathbf{x} \leq \mathbf{y}$ for every lower bound $\mathbf{x}$. It follows as above that if a greatest lower bound exist then it is unique. If a set $\mathbf{B}$ has a greatest lower bound $\mathbf{y}$, then we often write $\mathbf{y} = \text{G.L.B.}(\mathbf{B})$ or $\mathbf{x} = \mathbf{inf(B)}$. The symbolism **inf** is an

abbreviation for the quasi – Latin term for the greatest lower bound**;** namely**,** the *infimum***.**

Notice that the least upper bound is a lower bound for the set of upper bounds and a greatest lower bound is an upper bound for the set of lower bounds.

DEDEKIND COMPLETENESS AXIOM FOR THE REAL NUMBERS. *If* **A** *is a nonempty subset of* $\mathbb{R}$ *which has an upper bound, then* **A** *has a least upper bound.*

Corollary 2. *If* **B** *is a nonempty subset of* $\mathbb{R}$ *which has a lower bound, then* **B** *has a greatest lower bound.*

The proof of this corollary depends upon the following elementary observation**.**

Lemma 3. If **x** *and* **y** *are distinct real numbers and* $x < y$**,** *then* $-y < -x$**.**

***Proof of Lemma* 3.** By the axioms we know that $y - x > 0$**.** However**,** the left hand side is equal to $-(x - y)$**,** and therefore we have $-y < -x$ as required**.**

Proof of Corollary* 2.** Let **A** be the set of all ***negatives of elements of **B.** Then the assumption that **B** has a lower bound implies that A has an upper bound, and hence by the Dedekind Completeness Axiom the set **A** has a least upper bound, say **u.** We claim that $-u$ is a greatest lower bound for **B.** First of all**,** the lemma implies that since **u** is an upper bound for **A** the element $-u$ is a lower bound for **B.** Suppose now that **v** is an arbitrary lower bound for **B.** Then the lemma implies that $-v$ is an upper bound for **A,** and therefore since **u** is a least upper bound it follows that $u \leq -v$**.** Therefore the lemma implies that $v \leq -u$**,** so that $-u$ is a greatest lower bound for **B.**

Remarks. (1) If a set **A** does not have an upper bound, then this is often expressed symbolically as $\sup(A) = +\infty$**.** Notice that in this context the symbol "∞" is not a number, but rather It is a short way to say that there is no number which is an upper bound for **A.** Similarly**,** if **B** has no lower bound, then $\inf(B) = -\infty$**.**

(2) Two curious implications of the preceding notation are the "paradoxical" identities $\sup(\emptyset) = -\infty$ and $\inf(\emptyset) = +\infty$**.** To see the first of these**,** notice that every $M \in \mathbb{R}$ is an upper bound for the empty set**.** This holds because**,** given **M,** there is no $x \in \emptyset$ such that $x \geq M$**.** Therefore**,** the set of upper bounds for $\emptyset$ has no lower bound**.** To see the second**,** notice that every $M \in \mathbb{R}$ is a lower bound for the empty set**.** This holds because**,** given **M,** there is no $x \in \emptyset$ such that $x \leq M$**.** Therefore, the set of lower bounds for $\emptyset$ has no upper bound**.** — In contrast to this result**,** if **A** is a nonempty subset of **L** then we always have $\inf(A) \leq \sup(A)$ if we agree that $-\infty$ is less than every real number and $+\infty$ is greater than every real number (and of course $-\infty < +\infty$)**.** In fact**,** if **x** is an arbitrary element of **A** then we have $\inf(A) \leq x \leq \sup(A)$**.**

Clearly we want the real number system to contain the integers or a system equivalent to the integers. Here is one way of formulating this**:**

INTEGRAL COMPATIBILITY AXIOM. *There Is a* **1 – 1** *mapping* **J** *from the integers* $\mathbb{Z}$ *to the real numbers* $\mathbb{R}$ *with the following properties***:**

1. **J** *maps the zero element of* $\mathbb{Z}$ *to the zero element of* $\mathbb{R}$**.**
2. **J** *maps the multiplicative unit of* $\mathbb{Z}$ *to the multiplicative unit of* $\mathbb{R}$**.**
3. *For all integers* **x** *and* **y**, *we have* $\mathbf{J(x + y) = J(x) + J(y)}$**.**
4. *For all integers* **x** *and* **y**, *we have* $\mathbf{J(x\,y) = J(x)\,J(y)}$**.**
5. *For all integers* **x** *and* **y**, *we have* $\mathbf{J(x) < J(y)}$ *if and only if* $\mathbf{x < y}$**.**

Of course, the real numbers are also supposed to contain the ***rational numbers***, which are all numbers expressible as quotients of integers **a**/**b** where **b** is nonzero. Usually the rational numbers are denoted by $\mathbb{Q}$ (presumably for *quotients*). Note that the rational numbers clear satisfy all the properties of the real numbers aside from the Dedekind Completeness Property. Strictly speaking, we cannot say formally that this property fails for the rational numbers, but if we grant that there should be a real number that is the square root of 2, then an argument going back to the ancient Greeks (possibly even to the Pythagoreans in the 6th century B. C. E.) implies that some real numbers, including the square root of 2, are not rational. Incidentally, the classical number π, denoting the ration of a circle's circumference to its diameter, is also irrational, but this was first established in relatively modern times by J. H. Lambert (1728 – 1777); it should be noted that the first use of the symbol π for the number was due to W. Jones (1675 – 1749) in 1706. As noted at the beginning of these notes, one of the important features of set theory is that it provided a mathematically sound way of describing such irrational numbers as well as their relation to the rationals, thus completing the answer to a question that first arose in ancient Greek mathematics.

Uniqueness of the real numbers

We have given a list of properties that the real number system is assumed to satisfy. In the next section we shall prove that any system satisfying these properties also has many other familiar properties we expect from real numbers. However, as in Section 1 (and the discussion at the beginning of this unit), we would like to say that if we are given two systems which satisfy our axioms for the real numbers, then they are the same for all mathematical purposes; in the terminology of Section 1, the mathematical way of saying this is that there is an ***isomorphism*** between the two systems. Here is the formal statement.

Theorem 4. *Suppose that* **X** *and* **Y** *are sets with notions of addition, multiplication, ordering and "integers" which satisfy all the conditions for the real number system. Then there exists a* ***unique*** $\mathbf{1 - 1}$ *correspondence from* **h** *from* **X** *to* **Y** *that is an* ***isomorphism*** *in the sense of Section* **1**: *For all elements* $\mathbf{u, v \in X}$ *we have* $\mathbf{h(u + v) = h(u) + h(v)}$, $\mathbf{h(u \cdot v) = h(u) \cdot h(v)}$, *and* $\mathbf{h(u) < h(v)}$ *if and only if* $\mathbf{u < v}$. *Furthermore, the map* **h** *sends the zero and unit of* **X** *to the zero and unit of* **Y**, *and accordingly it also sends the "integers" in* **X** *to the "integers" in* **Y** *(and similarly for the "rationals" in the appropriate systems).*

By the "integers" in **X** and **Y** we mean the subsets described in the integral compatibility axiom, and the "rationals" denote the smallest subsets that are closed under addition, subtraction and multiplication and also contain both the integers and the reciprocals of nonzero integers.

As before, the existence of an isomorphism has the following implication:

> *Every true reasonable mathematical statement about the addition, multiplication and linear ordering of* **X** *is also true about* **Y** *and conversely.*

A proof of Theorem 4 appears in Unit **VIII.** The proof itself is relatively straightforward and elementary but somewhat tedious; however, it is absolutely necessary to establish such a result if we want to talk about **THE** real number system.

V. 5 : Familiar properties of the real numbers

(Lipschutz, §§ 2.2, 4.5)

The crucial justification for the Dedekind approach to the real number system is that it yields all the known properties of the real numbers. In this section we shall consider a few important examples:

Density of the rationals. *If* **x** *and* **y** *are rational numbers such that* $x < y$, *then there is a rational number* **q** *such that* $x < q < y$.

Existence of positive n^{th} ***roots.*** *If* **x** *is a positive real number and* **n** *is a positive integer, then there is a unique positive real number* **y** *such that* $y^n = x$.

Base* 10 *and decimal expansions. *The axioms for real numbers developed above are adequate to prove all the familiar facts about base* 10 *and infinite decimal expansions.*

A reasonable mathematical theory of the real numbers should be required to yield all of these properties in a fairly straightforward fashion.

As we have already noted, it is possible to go much further and develop everything done in calculus courses (and beyond!) using the given axioms for the real number system. Deriving all these fundamental results in calculus from our axioms is beyond the scope of these notes and this course (it properly belongs to courses on functions of a real variable); one standard reference which contains all the details is the following classic text:

> W. Rudin, ***Principles of Mathematical Analysis*** (3rd Ed.), International Series in Pure and Applied Mathematics). McGraw-Hill, New York, 1976. ISBN: 0 – 07 – 054235 – X.

We shall refer to Rudin at various points in this section as needed.

Density of the rational numbers

Even though numbers like the square root of 2 are irrational, it is still possible to approximate them to any desired degree of accuracy by rational numbers. This fact was

understood intuitively in most if not all ancient civilizations, and it was formalized and generalized by Eudoxus of Cnidus in the 4th century B. C. E.. Subsequently, Euclid's ***Elements*** used one formulation of this principle as the basis for its theory of geometric proportions. The first step in proving this rigorously for our formulation of the real numbers is named after Archimedes, who used it extensively in his writings during the 3rd century B. C. E., but it had also been known to Eudoxus and other earlier Greek mathematicians.

Theorem 1. (Archimedean Law) *If* $\mathbf{a}$ *and* $\mathbf{b}$ *are positive real numbers, then there is a positive integer* $\mathbf{n}$ *such that* $\mathbf{na > b}$.

By the well – ordering of the positive integers, there will be a ***(unique) minimal value*** of $\mathbf{n}$ for which this holds.

Proof. Assume the conclusion is false, so that for every positive integer $\mathbf{n}$ we have the inequality $\mathbf{na \leq b}$. If $\mathbf{A}$ denotes the set of all products $\mathbf{na}$, where $\mathbf{n}$ is a positive integer, it follows that $\mathbf{b}$ is an upper bound for $\mathbf{A}$, and by the Dedekind Completeness Property the set $\mathbf{A}$ must have a least upper bound, which we shall call $\mathbf{c}$. Since we have $\mathbf{ma \leq c}$ for every positive integer $\mathbf{m}$, if we set $\mathbf{m = n + 1}$ we see that $\mathbf{(n + 1)a \leq c}$ for every positive integer $\mathbf{n}$. If we subtract $\mathbf{a}$ from both sides, we see that $\mathbf{na \leq c - a}$ for every positive integer $\mathbf{n}$. But this implies that $\mathbf{c - a}$ is also an upper bound for $\mathbf{A}$, and we had chosen $\mathbf{c}$ to be the least upper bound, so we have obtained a contradiction. The latter arises from our assumption that $\mathbf{b}$ was an upper bound for $\mathbf{A}$, and therefore this must be false, which means that the conclusion of the theorem must be true.■

With this result at our disposal, we can prove the density of the rationals.

Theorem 2. *If* $\mathbf{a}$ *and* $\mathbf{b}$ *are positive real numbers such that* $\mathbf{a < b}$, *then there is a rational number* $\mathbf{q}$ *such that* $\mathbf{a < q < b}$.

One can easily obtain the same result when $\mathbf{a}$ and $\mathbf{b}$ are not both positive from the theorem as follows. If $\mathbf{a}$ is negative and $\mathbf{b}$ is positive, then we may simply take $\mathbf{q = 0}$. On the other hand, if $\mathbf{a < b < 0}$ then we have $\mathbf{-a > -b > 0}$, and therefore by the theorem there is a rational number $\mathbf{s}$ such that $\mathbf{-b < s < -a}$. If we take $\mathbf{q = -s}$, then it will follow that $\mathbf{a < q < b}$.

The proof of the theorem requires the following elementary facts.

Proposition 3. *If* $\mathbf{x}$ *is a positive real number, then its reciprocal* $\mathbf{x^{-1}}$ *is also positive.*

Proposition 4. *If* $\mathbf{x}$ *and* $\mathbf{y}$ *are positive real numbers such that* $\mathbf{x < y}$, *then their reciprocals satisfy the reverse inequalities* $\mathbf{x^{-1} > y^{-1}}$.

***Proof of Proposition* 3.** Suppose this is false, so that $\mathbf{x^{-1}}$ is negative. Then

$$\mathbf{-x^{-1} = (-1)x^{-1}}$$

Is positive, and therefore so is

$$\mathbf{-1 = x(-x^{-1}).}$$

Since the number $\mathbf{-1}$ is not positive we have a contradiction, which arises from our assumption that the reciprocal of $\mathbf{x}$ was negative, and therefore it follows that the reciprocal of $\mathbf{x}$ must be positive as claimed.■

Proof of Proposition 4. Suppose this is false, so that we have either $x^{-1} = y^{-1}$ or else $x^{-1} < y^{-1}$. The first of these implies that

$$y = xx^{-1}y = xy^{-1}y = x$$

which contradicts our assumption that $x < y$. To prove that $x^{-1} < y^{-1}$ is impossible, note first that if positive real numbers satisfy $a < b$ and $c < d$ then

$$bd - ac = (bd - ad) + (ad - ac) = (b - a)d + a(d - c) > 0$$

and hence $bd > ac$. Therefore $x < y$ and $x^{-1} < y^{-1}$ combine to imply that xx^{-1} is strictly less than yy^{-1}. However, each of the preceding two products is equal to 1 and thus we have a contradiction. Thus $x^{-1} < y^{-1}$ is impossible, and the only remaining possibility is the one stated in the conclusion of the result.■

Proof of Theorem 2. By Proposition 3, if a is positive then so is its reciprocal, and thus the Archimedean law implies there is some positive integer p such that $p = p \cdot 1 > a^{-1}$. Taking reciprocals, we find that $0 < 1/p < a$. The Archimedean Law similarly implies the existence of some positive integer r such that $0 < 1/r < b - a$. If we take m to be the larger of p and r, then it will follow that both $0 < 1/m < a$ and $0 < 1/m < b - a$. Applying the Archimedean Law one more time, we can find a ***first*** positive integer n such that $a < n/m$. If we also have $n/m < b$, then we may take $q = n / m$ and the proof will be complete. To see that $n/m < b$, proceed as follows. Since n is the first positive integer such that $a < n/m$, it follows that $(n - 1)/m \leq a$, and therefore we also have

$$n/m = \big((n - 1)/m\big) + (1/m) < a + (b - a) = b$$

which is exactly what we needed.■

A statement and proof of the Condition of Eudoxus are given in the online document

http://math.ucr.edu/~res/math153/history03a.pdf

and the application of the condition to proportionality questions as in Euclid's ***Elements*** appears in the following related document:

http://math.ucr.edu/~res/math153/history03b.pdf

Existence of positive n^{th} *roots*

The main result is exactly what we would expect:

Theorem 5. *If* r *is a positive real number and* $n > 1$ *is an integer, then there is a unique positive real number* y *such that* $y^n = r$.

The idea of the proof is simple. Given r and n, consider the set A of all positive real numbers y such that $y^n < r$. In order to prove the theorem, it will suffice to establish the following two points.

1. The set A has an upper bound (hence a least upper bound).
2. If z is the least upper bound of A, then $z^n = r$.

Proof of the first step. There are two separate cases, depending upon whether **r ≤ 1** or **r > 1.** In the first case, if **z** belongs to **A** then we also have **y ≤ 1,** for if **y > 1** then we have $z^n > 1$. Suppose now that **r > 1,** and let **n** be an integer such that **n > r.** We claim that **n** is an upper bound for **A;** as before, it suffices to show that if **y > n** then **y** does not belong to **A.** This follows because **z > n** and **n > 1** imply $z^n > n^n > n$.

The proof of the second step of Theorem 5 will rely on the following standard algebraic fact.

Theorem 6. (Binomial Theorem). *Let* **x** *and* **y** *be real numbers, and let* **n** *be a positive integer. Then we have*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

where the numbers

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

the usual binomial coefficients and **n!** denotes the factorial of **n,** which is formally defined by **0! = 1** *and the usual description for* **n > 0:**

$$n! = \prod_{k=1}^{n} k$$

The proof of this result proceeds by induction on **n** and is based upon the standard triangular identities named after B. Pascal (1623 – 1662), which state that

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

for non-negative integers **n** and **k** where **n ≥ k** and with the initial condition

$$\binom{n}{0} = \binom{n}{n} = 1.$$

In principle (at least), mathematicians in China and India had discovered the preceding identities centuries earlier, but we shall not elaborate on this point. Observe that if we take **x = y =** 1, then the formula states that the corresponding sum of binomial coefficients is equal to 2^n. We shall use this fact at a few steps in the proof of Theorem 5. Some of these steps will be stated separately before we proof the second part of Theorem 5.

Proofs of the Binomial Theorem appear in many precalculus and discrete structures textbooks (***e.g.***, see pages 327 – 328 of Rosen for an argument that is somewhat different from the inductive proof mentioned above), and therefore we shall not give a proof here.

Lemma 7. *If* **1 > t > 0** *then* $(1-t)^n > 1 - 2^n t$.

Lemma 8. *If* $1 > y > 0$ *and* $z > 1$ *then* $(z + y)^n < z^n + 2^n z^n y$, *and if* $1 > y > 0$ *and* $z < 1$ *then* $(z + y)^n < z^n + 2^n y$.

Proof of Lemma 7. In the Binomial Theorem take $x = 1$ and $y = -t$. Let $C(n, k)$ denote the (n, k) binomial coefficient to avoid typesetting problems. For each $k > 0$, a lower estimate for the k^{th} term of the expansion for $(1 - t)^n$ is given by $-C(n, k)t$. If we add these terms over all nonnegative values of k and use the fact that the sum of all the coefficients $C(n, k)$ is 2^n, we obtain the lower estimate in the statement of the lemma.■

Proof of Lemma 8. In this case we take $z = x$. Once again let $k > 0$. Then an upper estimate for the k^{th} term of the expansion is given by $C(n, k)z^n y$ if $z > 1$, and by the expression $C(n, k)y$ if $z < 1$. Adding these terms over all nonnegative values of k and using the fact that the sum of all the coefficients $C(n, k)$ is 2^n, we obtain the desired upper estimates.■

We are now prepared to complete the proof of the result on the existence of n^{th} roots.

Proof of the second part of Theorem 5. We again have separate cases where $r \leq 1$ or $r > 1$, and in each case we need to show that both $z^n < r$ and $z^n > r$ are impossible.

Before proceeding we make some elementary observations. If $r = 1$ then $z = 1$ and there is nothing to prove. We **CLAIM** that if $r < 1$ or $r > 1$ then z also satisfies $z < 1$ or $z > 1$ respectively. — If $r < 1$ then we claim there is a v such that $0 < v < 1$ and $v^n > r$. If this is true then r is an upper bound for S and therefore the least upper bound z must be strictly less than 1 (in fact, it must be strictly less than v). By Lemma 7 we know that if $1 > t > 0$ then $(1 - t)^n > 1 - 2^n$ and therefore if we choose v such that $x = 1 - v$ satisfies $2^n x < 1 - r$ then v^n will be strictly greater than r. Finally, if $r > 1$ then $r^{-1} < 1$, and hence there is some w such that $0 < w < 1$ and $w^n > r^{-1}$. If we set $v = w^{-1}$, we then obtain the inequalities $v > 1$ and $v^n < r$. But this means that $1 < v \leq z$.

Suppose now that $1 < r$ and $z^n < r$, where $z > 1$ by the preceding paragraph. If we have $w > z$ then $w^n \geq r$ because z is the least upper bound of all x such that $x^n < r$. Let $s = r - z^n$; it will suffice to find a number v such that v^n lies between z^n and r. If $1 > y > 0$ then Lemma 8 implies that $(z + y)^n$ is less than $z^n + 2^n z^n y$, and if we now choose y so that $2^n z^n y < s$, then $v = z + y$ will satisfy $z^n < v^n < r$. Now suppose we have $1 > r$ and $z^n < r$, so that $z < 1$ by the preceding paragraph. Let w and s be as before. Then we still have $w^n \geq r$ and we would again like to find some v such that $z^n < v^n < r$ and r. Taking y as before, we can use Lemma 8 to conclude that $(z + y)^n < z^n + 2^n y$, and if we choose y so that $2^n y < s$ then $v = z + y$ satisfies the desired condition $z^n < v^n < r$. Observe that the main difference in the arguments for the two cases $1 < r$ and $1 > r$ is the estimate for $(z + y)^n$ given by the Binomial Theorem.

Suppose now that $z^n > r$. By the definition of a least upper bound, for every $h > 0$ there is some w such that $z - w > h$ and $w^n < r$. Hence if $x < z$ and $h = z - x$ then we can find a w such that $x < w < z$ and $w^n < r$. The latter in turn implies that $x^n < w^n < r$. Thus we have shown that if $x < z$ then $w^n < r$, while if $x > z$ then $w^n > z^n > r$. Once again it will suffice to find a number v such that v^n lies between z^n and r. Let $s = z^n - r$ and let $y > 0$ as before, but now consider the quantity $(z - y)^n$. If $r > 1$ we then obtain the inequality

$$(z - y)^n > z^n - 2^n z^n y$$

while if $r > 1$ we obtain the inequality

$$(z + y)^n > z^n + 2^n y .$$

In each case if we choose **y** sufficiently small the right hand side will be strictly greater than **r**, which contradicts our previous observation that $x < z$ implies $w^n < r$. This completes the proof of Theorem 5.■

The next result is a simple consequence of Theorem 5 and the proof of Lemma **V.1.3**, but it provides an important relation between the algebraic and order structures on the real number system.

Corollary 8. *A real number* **x** *is nonnegative if and only if there is another real number* **y** *such that* $y^2 = x$.

Proof. The proof of Lemma **V.1.2** only depends upon algebraic and ordering properties that hold for both the integers and the real numbers, and thus it follows that Lemma **V.1.2** is also true for the real numbers; therefore for every real number **y** we see that the square y^2 is nonnegative. Conversely, by Theorem 5 we know that every nonnegative number is the square of some other real number.■

Section 4.5 of Lipschutz discusses the use of Theorem 5 to define rational and irrational powers of a positive real number (in particular, see the subheading, "Exponential Functions," at the bottom of page 101).

Base 10 *and decimal expansions*

We shall only summarize the main points here, leaving the proofs to an Appendix for this section of the notes.

One of the most elementary facts about a positive real number **x** is that it can be written as the sum $[x] + (x)$ of a nonnegative integer $[x]$ and a nonnegative real number (x) that is strictly less than one, and this decomposition is unique. The integer $[x]$ is often called the *greatest integer function* of **x** or the *integral part* of **x** or the *characteristic* of **x**, and the remaining number (x) is often called the *fractional part* or *mantissa* of **x**. The characteristic – mantissa terminology dates back to the original tables of base 10 logarithms published by H. Briggs (1561 – 1630); the literal meaning of the Latin root word ***mantisa*** is "makeweight," and it denotes something small that is placed onto a scale to bring the weight up to a desired value. We shall derive the decomposition of a nonnegative real number into a characteristic and mantissa from the axiomatic properties of the real numbers.

Theorem 9. *Let* **r** *be an arbitrary nonnegative real number. Then there is a unique decomposition of* **r** *as a sum* $n + s$, *where* **n** *is a nonnegative integer and* $0 \leq s < 1$.

Here is the standard result on ***base*** **N** or **N – *adic*** expansions of positive integers. In the standard case when $N = 10$, this yields the standard way of writing a nonnegative integer in terms of the usual Hindu – Arabic numerals, while if $n = 2$ or **8** or **16** this yields the binary or octal or hexadecimal expansion respectively.

Theorem 10. *Let* k *be a positive integer, and let* $N > 1$ *be another positive integer. Then there are unique integers* a_j *such that* $0 \le a_j \le N - 1$ *and*

$$k = a_0 + a_1 \cdot N + \ldots + a_m \cdot N^m$$

for a suitable nonnegative integer m.

For both practical and theoretical reasons, a mathematically sound definition of the real numbers should yield the usual decimal expansions for base 10 as well as the corresponding expansions for other choices of the base N. We shall verify this here and show that decimal expansions have several properties that are well – known from our everyday experience in working with decimals.

Although decimal expansions of real numbers are extremely useful for computational purposes, they are not particularly convenient for theoretical or conceptual purposes. For example, although every nonzero real number should have a reciprocal, describing this reciprocal completely and explicitly by infinite decimal expansions is awkward and generally unrealistic. Another difficulty is that decimal expansions are not necessarily unique; for example, the relation

$$1.0 = 0.99999999999999999999 \ldots$$

reflects the classical geometric series formula

$$a/(1 - r) = a + ar + ar^2 + \ldots + ar^k + \ldots$$

when $a = 9/10$ and $r = 1/10$. A third issue is whether one gets an equivalent number system if one switches from base 10 arithmetic to some other base. It is natural to expect that the answer to this question is yes, but any attempt to establish this directly runs into all sorts of difficulties almost immediately.

These are not just abstract, theoretical questions. The use of digital computers to carry out numerical computations implicitly assumes that one can work with real numbers equally well using infinite expansions with base 2 (or base 8 or 16 as in many computer codes, or even base 60 as in ancient Babylonian mathematics). One test of the usefulness of the abstract approach to real numbers is whether it yields such consequences and is base independent.

The preceding discussion justifies the standard method for expressing the integral part of a positive real number. Of course, the next step is to justify the standard expression for the fractional part. A natural first step is to verify that the usual types of infinite decimal expansions always yield real numbers.

Theorem 11. (Decimal Expansion Theorem). *Every infinite series of real numbers having the form*

$$a_N \cdot 10^N + a_{N-1} \cdot 10^{N-1} + \ldots + a_0 + b_1 \cdot 10^{-1} + b_2 \cdot 10^{-2} + \ldots + b_k \cdot 10^{-k} + \ldots$$

(*with* $0 \le a_i, b_j \le 9$)

is convergent. Conversely, every positive real number is the sum of an infinite series of this type where the coefficients of the powers of 10 *are integers satisfying the basic inequalities* $0 \le a_i, b_j \le 9$.

This turns out to be a fairly direct consequence of standard results on convergence of infinite series whose terms are all nonnegative (see Rudin, Theorem 3.25, page 60, for a proof):

COMPARISON TEST. *Suppose that*

$$\sum a_n \quad \text{and} \quad \sum b_n$$

are two series whose terms are nonnegative and satisfy $a_n < b_n$ *for all* n. *If the second series converges, then the first one does also.*

Theorem 10 immediately yields the standard "scientific notation" for a positive real number:

Corollary 12. (Scientific Notation Representation**).** *Every positive real number has a unique expression of the form* $a \cdot 10^M$, *where* $1 \le a < 10$ *and* M *is an integer.*

Decimal expansions of rational numbers

One basic test for the effectiveness of a mathematical theory is whether one can use it to shed light on patterns that run through many basic examples. The decimal expansions for rational numbers are an example of this type. If one computes the decimal expansions for some simple fractions, the results turn out to yield decimal expansions that are eventually repeating. Here are some examples:

1/3 = 0.33333333333333333333333333333333333 …
1/6 = 0.16666666666666666666666666666666666 …
1/7 = 0.14285714285714285714285714285714285 …
1/11 = 0.01010101010101010101010101010101010 …
1/12 = 0.08333333333333333333333333333333333 …
1/13 = 0.07692307692307692307692307692307692 …
1/17 = 0.05882352941176470588235294117647058 …
1/18 = 0.05555555555555555555555555555555555 …
1/19 = 0.05263157894736842105263157894736842 …
1/23 = 0.04347826086956521739130434782608695 …
1/27 = 0.03703703703703703703703703703703703 …
1/29 = 0.03448275862068965517241379310344827 5 …
1/31 = 0.03225806451612903225806451612903225 8 …
1/34 = 0.02941176470588235294117647058823529 4 …
1/37 = 0.02702702702702702702702702702702702 …

Motivated by such examples, it is natural to ask whether the decimal expansions for an arbitrary rational number must have the following special property:

Theorem 13. (Eventual Periodicity Property**).** *Suppose that* r *is a rational number such that* $0 < r < 1$, *and let*

$$r = b_1 \cdot 10^{-1} + b_2 \cdot 10^{-2} + \ldots + b_k \cdot 10^{-k} + \ldots$$

be a decimal expansion. Then the sequence $\{b_k\}$ *is* ***eventually periodic***; ***i.e.***, *there are positive integers* M *and* Q *such that* $b_k = b_{k+Q}$ *for all* $k > M$.

CONVERSELY, suppose that the statement in the claim holds for the decimal expansion of some number, and choose m and Q as above. Let s be given by the first $m - 1$

terms in the decimal expansion of **y,** and let **t** be the sum of the next **Q** terms**.** It then follows that **y** is equal to $s + t(1 + 10^{-Q} + 10^{-2Q} + 10^{-3Q} + \ldots)$**.** Now **s, t** and the geometric series in parentheses are all rational numbers**,** and therefore it follows that **y** is also a rational number**.** Therefore we have the following result**:**

Theorem 14. *A real number between* **0** *and* **1** *has a decimal expansion that is eventually periodic if and only if it is a rational number.*

Similar results hold if the numerical base **10** is replaced by an arbitrary integer $N > 1$**.**

Uniqueness properties of decimal expansions

Finally**,** here is the standard criterion for two decimal expressions to be equal**:**

Theorem 15. *Suppose that we are given two decimal expansions*

$$a_N \cdot 10^N + a_{N-1} \cdot 10^{N-1} + \ldots + a_0 + b_1 \cdot 10^{-1} + b_2 \cdot 10^{-2} + \ldots + b_k \cdot 10^{-k} + \ldots$$

$$c_N \cdot 10^N + c_{N-1} \cdot 10^{N-1} + \ldots + c_0 + d_1 \cdot 10^{-1} + d_2 \cdot 10^{-2} + \ldots + d_k \cdot 10^{-k} + \ldots$$

which yield the same real number. Then $a_j = c_j$ *for all* **j***, and (exactly) one of the following mutually exclusive statements is also true***:**

(1) *For each* **k** *we have* $b_k = d_k$**.**

(2) *There is an* $L > 0$ *such that* $b_k = d_k$ *for every* $k < L$ *but* $b_{L+1} = d_L + 1$**,** *with* $b_k = 0$ *for* $k > L$ *and* $d_k = 9$ *for all* $k > L$**.**

(3) *There is an* $L > 0$ *such that* $b_k = d_k$ *for every* $k < L$ *but* $d_{L+1} = b_L + 1$**,** *with* $d_k = 0$ *for* $k > L$ *and* $b_k = 9$ *for all* $k > L$ *(the analog of the previous possibility with the roles of the two expansions switched).*

One can reformulate the preceding into a strict uniqueness result as follows**:**

Corollary 16. *Every positive real number has a unique decimal expansion of the form*

$$a_N \cdot 10^N + a_{N-1} \cdot 10^{N-1} + \ldots + a_0 + b_1 \cdot 10^{-1} + b_2 \cdot 10^{-2} + \ldots + b_k \cdot 10^{-k} + \ldots$$

such that b_k *is nonzero for infinitely many choices of* **k.**

EXAMPLE. We can use the preceding result to define real valued functions on an interval in terms of decimal expansions**.** In particular**,** if we express an arbitrary real number $x \in (0, 1]$ as an infinite decimal

$$x = 0.b_1 b_2 b_3 b_4 b_5 b_6 b_7 b_8 b_9 \ldots$$

where infinitely many digits b_k are nonzero, then we may define a function **f** from $(0, 1]$ to itself by the formula

$$f(x) = 0.b_1 0 b_2 0 b_3 0 b_4 0 b_5 0 b_6 0 b_7 0 b_8 0 b_9 0 \ldots$$

and if we extend this function by setting $f(0) = 0$ then we obtain a strictly increasing function on the closed unit interval (verify that the function is strictly increasing**!**)**.** Note that this function has a jump discontinuity at every finite decimal fraction**.**

Since every nondecreasing real valued function on a closed interval is Riemann integrable, we know that **f** can be integrated. It turns out that the value of this integral is a fairly simple rational number; finding the precise value is left as an exercise for the reader (this is a good illustration of the use of Riemann sums — a natural strategy is to partition the unit interval into pieces whose endpoints are finite decimal fractions with at most **n** nonzero terms and to see what happens to the Riemann sums as **n** increases).

V. 5. Appendix A : Proofs of results on number expansions

This appendix contains proofs of several results from Section 5:

We begin by proving that a positive real number can be written in an essentially unique manner as the sum of an integral part and a fractional part which lies between 0 and 1.

Theorem V.5.9. *Let* **r** *be an arbitrary nonnegative real number. Then there is a unique decomposition of* **r** *as a sum of the form* $\mathbf{n} + \mathbf{s}$ *such that* **n** *is a nonnegative integer and* $0 \leq \mathbf{s} < 1$.

Proof. By the Archimedean Law there is a nonnegative integer **m** such that $\mathbf{m} > \mathbf{r}$, and since the nonnegative integers are well – ordered there is a ***minimum*** such integer $\mathbf{m_1}$. Since **r** is nonnegative it follows that $\mathbf{m_1}$ cannot be zero and hence must also be positive. Therefore $\mathbf{m_1 - 1}$ is also nonnegative and by the minimal nature of the positive integer $\mathbf{m_1}$ we must have $\mathbf{m_1 - 1 \leq r}$. If we take $\mathbf{n = m_1 - 1}$ and $\mathbf{s = r - n}$ then $\mathbf{r = n + s}$ where **n** and **s** have the desired properties. Suppose that we also have $\mathbf{r = q + v}$, where **q** is a nonnegative integer and $\mathbf{0 \leq q < 1}$. By hypothesis we have

$$\mathbf{q \leq r < q + 1}$$

and the right hand inequality implies $\mathbf{n + 1 \leq q + 1}$, or equivalently $\mathbf{n \leq q}$. The equation $\mathbf{r = n + s = q + v}$ can therefore be rewritten in the form

$$\mathbf{0 \leq q - n = s - v}$$

and since ***(i)*** $\mathbf{s - v \leq s < 1}$ and ***(ii)*** $\mathbf{q - n}$ is an integer, it follows that $\mathbf{n = q}$ and $\mathbf{s = v}$.■

Base **N** *expansions for natural numbers*

We shall use the long division property for natural numbers to derive the standard result on base **N** expansions of positive integers**.** In the standard case when **N = 10,** this yields the standard way of writing a nonnegative integer**.**

Theorem V.5. 10. *Let* **k** *be a positive integer, and let* **N > 1** *be another positive integer. Then there are unique integers* a_j *such that* $0 \leq a_j \leq N - 1$ *and*

$$k = a_0 + a_1 N + \ldots + a_m N^m$$

for a suitable nonnegative integer **m.**

In the course of proving this result it will be useful to know the following**:**

Lemma 1. *Suppose that integers* **N, k,** *and* a_j *are given as above. Then we have*

$$a_0 + a_1 N + \ldots + a_m N^m \leq N^{m+1}.$$

Proof of Lemma 1. Since $a_j \leq N - 1$ for each **j** we have

$$a_j N^j \leq (N-1)N^j = N^{j+1} - N^j$$

and therefore we have the inequality

$$a_0 + a_1 N + \ldots + a_m N^m \leq (N-1) + (N^2 - N) + \ldots + (N^{m+1} - N^m) = N^{m+1} - 1 < N^{m+1}.\blacksquare$$

Proof of Theorem V.5. 10. It is always possible to find an exponent **q** such that $2^q > k$**,** and since $k \geq 2$ it follows that we also have $N^q > 2^q > k$**.** Let $[S_m]$ be the statement of the statement that every positive integer less than N^{m+1} has a unique expression as above**.** If $m = 0$ then the result follows immediately from the long division theorem**,** for then $k = a_0$**.** Suppose now that $[S_{p-1}]$ is true and consider the statement $[S_p]$**.** If $k < N^{p+1}$ then we can use long division to write **k** uniquely in the form

$$k = k_0 + a_p N^p$$

where $a_p \geq 0$ and $0 \leq k_0 < N^p$**.** We claim that $a_p < N$**.** If this were false then we would have $k \geq a_p N^p \geq N N^p = N^{p+1}$**,** contradicting the assumption $k < N^{p+1}$**.**

By induction we know that k_0 has a unique expression as a sum

$$k_0 = a_0 + a_1 N + \ldots + a_{p-1} N^{p-1}$$

for suitable a_j**.** This proves existence**.** To prove uniqueness**,** suppose that we have

$$k = a_0 + a_1 N + \ldots + a_p N^p = b_0 + b_1 N + \ldots + b_p N^p.$$

Denote all but the last terms of these sums by $A = a_0 + a_1 N + \ldots + a_{p-1} N^{p-1}$ and $B = b_0 + b_1 N + \ldots + b_{p-1} N^{p-1}$**.** Then we have $0 \leq A, B \leq N^p - 1$ by the lemma, and therefore by the uniqueness of the long division expansion of k it follows that $a_p = b_p$ and $A = B$**.** By the induction hypothesis the latter implies that $a_j = b_j$ for all $j < p$**.** Therefore we have also shown uniqueness**.**$\blacksquare$

Decimal expansions for real numbers

As we have already noted, a mathematically sound definition of the real numbers should yield the usual decimal expansions for base **10** as well as the corresponding expansions for other choices of the base **N.** We shall verify this and show that decimal expansions have many properties that are more or less predictable on empirical grounds.

One such property is the well – known decimal equality **1.0 = 0.9999999 ...** so we begin by noting this reflects the geometric series formula

$$a/(1-r) = a + ar + ar^2 + \ldots + ar^k + \ldots$$

when $a = 9/10$ and $r = 1/10$. In fact, the geometric series plays a key role in proving that infinite decimal expansions always yield real numbers.

Theorem V.5. 11 (Decimal Expansion Theorem**).** *Every infinite series of real numbers having the form*

$$a_N \cdot 10^N + a_{N-1} \cdot 10^{N-1} + \ldots + a_0 + b_1 \cdot 10^{-1} + b_2 \cdot 10^{-2} + \ldots + b_k \cdot 10^{-k} + \ldots$$

(*with* $0 \le a_i, b_j \le 9$)

is convergent. Conversely, every positive real number is the sum of an infinite series of this type where the coefficients of the powers of **10** *are integers satisfying the basic inequalities* $0 \le a_i, b_j \le 9$.

As noted above, there are two ways of writing **1** as an infinite series of this type, so such a representation is not unique, but empirical evidence suggest that all ambiguities in decimal expansions arise from this example, and we shall verify this later.

PROOF OF THE DECIMAL EXPANSION THEOREM. The proof of this result splits naturally into two parts, one for each implication direction.

Formal infinite decimal expansions determine real numbers: If one can show this for positive decimal expansions, it will follow easily for negative ones as well, so we shall restrict attention to the positive case. Consider the formal expression given above:

$$(a_N \cdot 10^N + a_{N-1} \cdot 10^{N-1} + \ldots + a_0 + b_1 \cdot 10^{-1} + b_2 \cdot 10^{-2} + \ldots + b_k \cdot 10^{-k} + \ldots)$$

For each integer $p > 0$, define s_p to be the sum of all terms in this expression up to and including $b_p 10^{-p}$ and let **S** be the set of all such numbers s_p. Then the set **S** has an upper bound, and in fact we claim that 10^{N+1} is an upper bound for **S.** To see this, observe that $a_N \cdot 10^N + a_{N-1} \cdot 10^{N-1} + \ldots + a_0 \le 10^{N+1} - 1$ by a previous lemma and

$$b_1 \cdot 10^{-1} + b_2 \cdot 10^{-2} + \ldots + b_k \cdot 10^{-k} + \ldots \le$$
$$9 \cdot (10^{-1} + 10^{-2} + \ldots + 10^{-k} + \ldots) = 1$$

and the assertion about an upper bound follows immediately from this. The least upper bound **r** for **S** turns out to be the limit of the sequence of partial sums $\{s_p\}$.

Real numbers determine infinite decimal expansions: Given (say) a positive real number **r**, the basic idea is to find a sequence of finite decimal fractions $\{s_p\}$ such that for every value of **p** the number s_p is expressible as a fraction whose denominator is given by 10^p and

$$s_p \le r < s_p + 10^{-p}.$$

More precisely, suppose that we already have s_p and we want to find the next term. By construction $10^p s_p$ is a positive integer and $10^p s_p \le 10^p r < 10^p s_p + 1$, so that

$$10^{p+1} s_p \le 10^{p+1} r < 10^{p+1} s_p + 10.$$

Choose b_{p+1} to be the largest integer such that

$$b_{p+1} \le 10^{p+1} r - 10^{p+1} s_p.$$

The right hand side is positive so this means that $b_{p+1} \ge 0$. On the other hand, the previous inequalities also show that $b_{p+1} < 10$ and since b_{p+1} is an integer this implies $b_{p+1} \le 9$. If we now take $s_{p+1} = 10 s_p + b_{p+1}$ then it will follow that

$$s_{p+1} \le r < s_{p+1} + 10^{-(p+1)}.$$

To see that the sequence converges, note that it corresponds to the infinite series

$$s_p + \sum_p (b_{p+1} 10^{-p}),$$

which converges by comparison with the modified geometric series $s_p + \sum_p 10^{(1-p)}$.■

Corollary V.5.12 (Scientific Notation Representation**).** *Every positive real number has a unique expansion of the form* $a \cdot 10^M$, *where* $1 \le a < 10$ *and* M *is an integer.*

Existence. If x has the decimal expansion

$$a_N \cdot 10^N + a_{N-1} \cdot 10^{N-1} + \ldots + a_0 + b_1 \cdot 10^{-1} + b_2 \cdot 10^{-2} + \ldots + b_k \cdot 10^{-k} + \ldots$$

(*with* $0 \le a_i, b_j \le 9$)

then $x \cdot 10^{-N}$ lies in the interval $[1, 10)$ by construction.

Uniqueness. Suppose that we can write x as $a \cdot 10^M$ and $b \cdot 10^N$. Then by the conditions on the coefficients, we know that $x \in [10^M, 10^{M+1}) \cap [10^N, 10^{N+1})$. Since the half open intervals $[10^M, 10^{M+1})$ and $[10^N, 10^{N+1})$ are disjoint unless $M = N$, it follows that the latter must hold. Therefore the equations $x = a \cdot 10^M = b \cdot 10^N$ and $M = N$ imply $a = b$.■

Decimal expansions of rational numbers

In working with decimals one eventually notices that the decimal expansions for rational numbers have the following special property:

Theorem V.5.13 (Eventual Periodicity Property**).** *Suppose that* r *is a rational number such that* $0 < r < 1$, *and let*

$$r = b_1 \cdot 10^{-1} + b_2 \cdot 10^{-2} + \ldots + b_k \cdot 10^{-k} + \ldots$$

be a decimal expansion. Then the sequence $\{b_k\}$ *is* ***eventually periodic****; i.e., there are positive integers* M *and* Q *such that* $b_k = b_{k+Q}$ *for all* $k > M$.

Proof. Let a/b be a rational number between **0** and **1,** where **a** and **b** are integers satisfying $0 < a < b$. Define sequences of numbers r_n and x_n recursively, beginning with $r_0 = a$ and $x_0 = 0$. Given r_n and x_n express the product $10\,r_n$ by long division in the form $10\,r_n = b\,x_{n+1} + r_{n+1}$ where $x_{n+1} \geq 0$ and $0 \leq r_{n+1} < b$.

CLAIMS:

1. *Both of these numbers only depend upon* r_n.
2. *We have* $x_{n+1} < 10$.

The first part is immediate from the definition in terms of long division, and to see the second note that $x_{n+1} \geq 10$ would imply $10\,r_n \geq 10\,b$, which contradicts the fundamental remainder condition $r_n < b$.

Since r_n can only take integral values between **0** and $b - 1$, it follows that there are some numbers **Q** and **m** such that $r_m = r_{m+Q}$.

CLAIM: $r_k = r_{k+Q}$ *for all* $k \geq m$.

We already know this for $p = m$, so assume it is true for $p \leq k$. Now each term in the sequence r_n depends only on the previous term, and hence the relation $r_k = r_{k+Q}$ implies $r_{k+1} = r_{k+Q+1}$. Therefore the claim is true by finite induction.■

CONVERSELY, suppose that the statement in the claim holds for the decimal expansion of some number, and choose **m** and **Q** as above. Let **s** be given by the first $m - 1$ terms in the decimal expansion of **y**, and let **t** be the sum of the next **Q** terms. It then follows that **y** is equal to $s + t\,(1 + 10^{-Q} + 10^{-2Q} + 10^{-3Q} + \ldots)$. Now **s, t** and the geometric series in parentheses are all rational numbers, and therefore it follows that **y** is also a rational number. Therefore we have the following result:

Theorem V.5.14. *A real number between* **0** *and* **1** *has a decimal expansion that is eventually periodic if and only if it is a rational number.*■

In Section 5 we gave the following examples to illustrate the theorem:

$$
\begin{aligned}
1/3 &= 0.33333333333333333333333333333333333333\ldots\\
1/6 &= 0.16666666666666666666666666666666666666\ldots\\
1/7 &= 0.14285714285714285714285714285714285714\ldots\\
1/11 &= 0.01010101010101010101010101010101010101\ldots\\
1/12 &= 0.08333333333333333333333333333333333333\ldots\\
1/13 &= 0.07692307692307692307692307692307692307\ldots\\
1/17 &= 0.05882352941176470588235294117647058823\ldots\\
1/18 &= 0.05555555555555555555555555555555555555\ldots\\
1/19 &= 0.05263157894736842105263157894736842105\ldots\\
1/23 &= 0.04347826086956521739130434782608695652\ldots\\
1/27 &= 0.03703703703703703703703703703703703703\ldots\\
1/29 &= 0.03448275862068965517241379310344827586\ldots\\
1/31 &= 0.03225806451612903225806451612903225806\ldots\\
1/34 &= 0.02941176470588235294117647058823529411\ldots\\
1/37 &= 0.02702702702702702702702702702702702702\ldots
\end{aligned}
$$

Note that the minimal period lengths in these examples are **1, 1, 6, 2, 1, 6, 16, 1, 18, 22, 3, 28, 15, 16** and **3.** One is naturally led to the following question**:**

Given a fraction **a/b** *between* **0** *and* **1,** *what determines the (minimal) period length* **Q?**

To illustrate the ideas**,** we shall restrict attention to the special case where **a/b = 1/p,** where **p** is a prime not equal to **2** or **5** (the two prime divisors of **10**)**.** In this case the methods of abstract algebra yield the following result**:**

Theorem 2. *If* **p ≠ 2, 5** *is a prime, then the least period* **Q** *for the decimal expansion of* **1/p** *is equal to the multiplicative order of* **10** *in the (finite cyclic) group of multiplicative units for the integers mod* **p.**■

We shall not verify this result here, but the proof is not difficult**.**

Corollary 3. *The least period* **Q** *divides* **p – 1.**

The corollary follows because the order of the group of units is equal to **p – 1** and the order of an element in a finite group always divides the order of the group**.**■

One is now led to ask when the period is actually equal to this maximum possible value**.** Our examples show this is true for the primes **7, 19, 23** and **29** but not for the primes **11, 13, 31** or **37.**

More generally**,** one can define a primitive root of unity in the integers mod **p** to be an integer **a** mod **p** such that **a** is not divisible by **p** and the multiplicative order of the class of **a** in the integers mod **p** is precisely **p – 1.** Since the group of units is cyclic**,** such primitive roots always exist**,** and one can use the concept of primitive root to rephrase the question about maximum periods for decimal expansions in the following terms**:**

For which primes **p** *is* **10** *a primitive root of unity mod* **p?**

A simple answer to this question does not seem to exist**.** In the 1920s E. Artin (1898 – 1962) stated the following conjecture**:**

Every integer **a > 1** *is a primitive root of unity mod* **p** *for infinitely many primes* **p.**

This means that **10** ***should*** be the primitive root for infinitely many primes **p,** and hence there should be infinitely many full – period primes**.** Quantitatively**,** the conjecture amounts to showing that about **37%** of all primes asymptotically have **10** as primitive root**.** The percentage is really an approximation to Artin's constant

$$C_{\text{Artin}} = \prod_{k=1}^{\infty}\left[1 - \frac{1}{p_k(p_k-1)}\right] = 0.3739558136\ldots$$

where $\mathbf{p_k}$ denotes the $\mathbf{k^{th}}$ prime**.** Further information about this number and related topics appears in the following online reference**:**

http://mathworld.wolfram.com/ArtinsConstant.html

Uniqueness of decimal expansions

The criterion for two decimal expressions to be equal is well understood**.**

Theorem V.5. 15. *Suppose that we are given two decimal expansions*

$$a_N \cdot 10^N + a_{N-1} \cdot 10^{N-1} + \ldots + a_0 + b_1 \cdot 10^{-1} + b_2 \cdot 10^{-2} + \ldots + b_k \cdot 10^{-k} + \ldots$$

$$c_N \cdot 10^N + c_{N-1} \cdot 10^{N-1} + \ldots + c_0 + d_1 \cdot 10^{-1} + d_2 \cdot 10^{-2} + \ldots + d_k \cdot 10^{-k} + \ldots$$

which yield the same real number. Then $a_j = c_j$ *for all* j*, and (exactly) one of the following mutually exclusive statements is also true*:

(1) *For each* k *we have* $b_k = d_k$.

(2) *There is an* $L > 0$ *such that* $b_k = d_k$ *for every* $k < L$ *but* $b_{L+1} = d_L + 1$, *with* $b_k = 0$ *for* $k > L$ *and* $d_k = 9$ *for all* $k > L$.

(3) *There is an* $L > 0$ *such that* $b_k = d_k$ *for every* $k < L$ *but* $d_{L+1} = b_L + 1$, *with* $d_k = 0$ *for* $k > L$ *and* $b_k = 9$ *for all* $k > L$ *(the analog of the previous possibility with the roles of the two expansions switched).*

If x and y are given by the respective decimal expansions above, then $x = y$ implies the greatest integer functions satisfy $[x] = [y]$, which in turn implies that $a_j = c_j$ for all j. Furthermore, we then also have $(x) = (y)$ and accordingly the proof reduces to showing the result for numbers that are between 0 and 1.

The following special uniqueness result will be helpful at one point in the general proof.

Lemma 4. *For each positive integer* k *let* t_k *be an integer between* 0 *and* 9. *Then we have*

$$1 = t_1 \cdot 10^{-1} + t_2 \cdot 10^{-2} + \ldots + t_k \cdot 10^{-k} + \ldots$$

if and only if $t_k = 9$ *for all* k.

Proof. Let t be the summation on the right hand side. If $t_k = 9$ for all k then $t = 1$ by the geometric series formula. Conversely, if $t_m < 9$ for a specific value of m then

$$t_1 \cdot 10^{-1} + t_2 \cdot 10^{-2} + \ldots + t_k \cdot 10^{-k} + \ldots < u_1 \cdot 10^{-1} + u_2 \cdot 10^{-2} + \ldots + u_k \cdot 10^{-k} + \ldots$$

where $u_k = 9$ for $k \neq m$ and $u_m \leq 8$. The latter implies that the right hand side is less than or equal to $1 - 10^{-m}$, which is strictly less than 1.■

Theorem 5. *If we are given two decimal expansions*

$$x = x_1 \cdot 10^{-1} + x_2 \cdot 10^{-2} + \ldots + x_k \cdot 10^{-k} + \ldots$$

$$y = y_1 \cdot 10^{-1} + y_2 \cdot 10^{-2} + \ldots + y_k \cdot 10^{-k} + \ldots$$

then $x = y$ *if and only if one of the following is true*:

(1) *For all positive integers* k *we have* $x_k = y_k$.

(2) *There is some positive integer* M *such that* **[i]** $x_k = y_k$ *for all* $k < M$, **[ii]** $x_M = y_M + 1$, **[iii]** $x_k = 0$ *for* $k > M$, *and* **[iv]** $y_k = 9$ *for* $k > M$.

(3) *A statement analogous to* **(2)** *holds in which the roles of* x_k *and* y_k *are switched*; *namely, there is a positive integer* M *such that* **[i]** $y_k = x_k$ *for all* $k < M$, **[ii]** $y_M = x_M + 1$, **[iii]** $y_k = 0$ *for* $k > M$, *and* **[iv]** $x_k = 9$ *for* $k > M$.

Proof. Suppose that the first alternative does not happen, and let L be the first positive integer such that $x_L \neq y_L$. Without loss of generality, we may as well assume that the inequality is $x_L > y_L$ (if the inequality points in the opposite direction, then one can apply the same argument reversing the roles of x_k and y_k throughout). Let z be given by the first $L - 1$ terms of either x or y (these are equal).

CASE 1. Suppose that $x_L \geq y_L + 2$. Note that $y_L \leq 7$ is true in this case. We then have

$$y \leq z + 10^{-L} y_L + 9 \cdot 10^{-L}(10^{-1} + 10^{-2} + \ldots + 10^{-k} + \ldots) =$$

$$z + 10^{-L}(y_L + 1) < z + 10^{-L}(x_L) \leq$$

$$z + 10^{-L}(x_L + x_{L+1}10^{-1} + x_{L+2}10^{-2} + \ldots + x_{L+k}10^{-k} + \ldots) = x.$$

Therefore $x > y$ if we have $x_L \geq y_L + 2$.

CASE 2. Suppose that $x_L = y_L + 1$, and let $w = 10^{-L} y_L$, so that $x_L = w + 10^{-L}$. We may then write

$$x = z + (w + 10^{-L}) + 10^{-L} u \quad \text{and} \quad y = z + w + 10^{-L} v$$

where by construction u and v satisfy $0 \leq u, v \leq 1$. If $x = y$ then the displayed equations imply that $10^{-L} + 10^{-L} u = 10^{-L} v$. The only way such an equation can hold is if $u = 0$ and $v = 1$. The first of these implies that the decimal expansion coefficients for the sum

$$0 = u = x_{L+1}10^{-1} + x_{L+2}10^{-2} + \ldots + x_{L+k}10^{-k} + \ldots$$

must satisfy $x_k = 0$ for all $k > L$, and by the lemma the second of these can only happen if the decimal expansion coefficients for the sum

$$1 = v = y_{L+1}10^{-1} + y_{L+2}10^{-2} + \ldots + y_{L+k}10^{-k} + \ldots$$

satisfy $y_k = 9$ for all $k > L$. Therefore the second alternative holds in Case 2.

Conversely, the standard geometric series argument shows that two numbers with decimal expansions given by the second or third alternatives must be equal. Of course, the two numbers are equal if the first alternative holds, so this completes the proof of the theorem.■

One can reformulate the preceding into a strict uniqueness result as follows:

Corollary V.5. 16. *Every positive real number has a unique decimal expansion of the form*

$$a_N \cdot 10^N + a_{N-1} \cdot 10^{N-1} + \ldots + a_0 + b_1 \cdot 10^{-1} + b_2 \cdot 10^{-2} + \ldots + b_k \cdot 10^{-k} + \ldots$$

such that b_k *is nonzero for infinitely many choices of* k.

This follows immediately from the preceding results on different ways of expressing the same real number in decimal form; there is more than one way of writing a number in decimal form if and only if it is an integer plus a finite decimal fraction, and in this case there is only one other way of doing so and all, but finitely many digits of the alternate expansion are equal to 9.■

VI : Infinite constructions in set theory

In elementary accounts of set theory, examples of finite collections of objects receive a great deal of attention for several reasons. For example, they provide relatively simple illustrations of the abstract formal concepts in the subject. However, Cantor's original motivation for studying set theory involved ***infinite*** collections of objects, and the real breakthrough of set theory was its ability to provide a framework for studying infinite collections and limits that were previously difficult or out of reach.

We shall begin with a variation on the material in Section **III.3**, describing unions and intersections of ***indexed families*** of sets; a typical example of this sort is a sequence of sets $\mathbf{A_n}$, where **n** runs through all positive integers. In the second section we define a notion of (possibly infinite) ***Cartesian product for*** such ***indexed families.*** This definition has some aspects that may seem unmotivated, and therefore we shall also describe an axiomatic approach to products such that (i) there is essentially only one set – theoretic construction satisfying the axioms, (ii) the construction in these notes satisfies the axioms. In the next two sections we shall present Cantor's landmark results on comparing infinite sets, including proofs of the following,

1. There is a $\mathbf{1-1}$ correspondence between the nonnegative integers $\mathbb{N}$ and the integers $\mathbb{Z}$.
2. There is a $\mathbf{1-1}$ correspondence between the nonnegative integers $\mathbb{N}$ and the rational numbers $\mathbb{Q}$.
3. There is **NO** $\mathbf{1-1}$ correspondence between the nonnegative integers $\mathbb{N}$ and the real numbers $\mathbb{R}$.

We should note that a few aspects of Cantor's discoveries (in particular, the first of the displayed statements) had been anticipated three centuries earlier by Galileo.

Section 5 is a commentary on the impact of set theory, and Section 6 looks at generalizations of finite induction and recursion for sets that are larger than the natural numbers $\mathbb{N}$. The latter is included mainly as background for the sake of completeness.

VI.1 : Indexed families and set – theoretic operations

(Halmos, §§ 4, 8 – 9; Lipschutz, §§ 5.3 – 5.4)

One can summarize this section very quickly as follows: In Unit **III** we introduced several ways of constructing a third set out of two given ones, and in this section we shall describe similar ways of constructing a new set out of a more or less arbitrary list of other ones.

We have frequently considered finite and infinite sequences of sets having the form $\mathbf{A_n}$ where the indexing subscript **n** runs through some finite or infinite set **S** of nonnegative integers. Formally, such a sequence of sets corresponds to a function for which the value at a given integer **n** in **S** is equal to $\mathbf{A_n}$. We can generalize this as follows:

Definition. Let $\mathbf{I}$ be a set. An ***indexed family of sets with indexing set*** $\mathbf{I}$ is a function from $\mathbf{I}$ to some other set **X;** very often **X** is the set **P(Y)** of subsets of some other set **Y.** Such an indexed family is usually described by notation such as $\mathbf{\{A_i\}_{i \in I}}$. In such cases $\mathbf{I}$ is generally called the ***index set***, while $\mathbf{I(i) = A_i}$ is the ***mapping*** or (Halmos' terminology) ***family,*** and $\mathbf{A_i}$ is the ***element belonging to the index value*** **i,** which is sometimes also called the $\mathbf{i^{th}}$ ***element*** or ***term of the indexed family.***

Given any sort of mathematical objects (***e.g.***, partially ordered sets), one can define an indexed family of such objects similarly.

As indicated on page 34 of Halmos, in mathematical writings the notation for an indexed family is often abbreviated to $\mathbf{\{A_i\}}$, and this is described by the phrase, "unacceptable but generally accepted way of communicating the notation and indicating the emphasis." A more concise description would be a "slight abuse of language." Such an abbreviation should only be used if the indexing set it obvious from the context (for example, a subscript of **n** almost always denotes an integer) or its precise nature is relatively unimportant and there is no significant danger that the notation will be misinterpreted.

Subfamilies. An indexed family $\mathbf{\{B_i\}_{i \in J}}$ is a ***subfamily*** of a family of $\mathbf{\{A_i\}_{i \in I}}$, if and only if $\mathbf{J}$ is a subset of $\mathbf{I}$ and for all **i** in $\mathbf{J}$ we have $\mathbf{B_i = A_i}$.

Indexed unions and intersections

Given a set **C,** in Unit $\mathbf{III}$ we considered the union **$(C),** which is the collection of all **x** such that $\mathbf{x \in A}$ for some $\mathbf{A \in C}$, and we introduced the usual ways of writing these sets as $\mathbf{\cup\{A \mid A \in C\}}$ or $\mathbf{\cup_{A \in C} A}$. If we have an indexed family of sets $\mathbf{\{A_i\}_{i \in I}}$, then the ***indexed union***

$$\bigcup_{i \in I} A_i,$$

will refer to the union of the collection $\mathbf{\{B \mid B = A_i}$ for some $\mathbf{i \in I\}}$. Recall that here $\mathbf{I}$ is a set, and $\mathbf{A_i}$ is a set for every $\mathbf{i \in I}$. In the case that the index set $\mathbf{I}$ is the set of natural numbers, one also uses notation is analogous to that of infinite series:

$$\bigcup_{i=1}^{\infty} A_i.$$

Similarly, given a ***nonempty*** set **C** (recall the extra condition is important!), in Unit $\mathbf{III}$ we considered the intersection of the sets in **C,** which is the set of all **x** such that $\mathbf{x \in A}$ for every $\mathbf{A \in C}$, and we similarly introduced the analogous ways of writing these sets

as $\cap\{A \mid A \in C\}$ or $\cap_{A \in C} A$. If we have an indexed family of sets $\{A_i\}_{i \in I}$, then we also have the corresponding indexed intersection

$$\bigcap_{i \in I} A_i.$$

As one might expect, this will be the intersection of the indexed collection $\{ B \mid B = A_i$ for some $i \in I \}$. As before, in the case that the index set I is the set of natural numbers, one also uses notation is analogous to that infinite series:

$$\bigcap_{i \in I} A_i.$$

These indexed unions and intersections satisfy analogs of the basic formal properties of ordinary unions and intersections which are stated formally on pages 35 – 36 of Halmos.

Numerous properties of unions and intersections of indexed families are developed in the exercises.

VI.2 : Infinite Cartesian products

(Halmos, § 9; Lipschutz, §§ 5.4, 9.2)

We have already considered **n – *fold Cartesian products*** of **n** sets $X_1, \ldots, X_n$:

$$X_1 \times \ldots \times X_n = \{ (x_1, \ldots, x_n) \mid x_1 \in X_1 \ \& \ \ldots \ \& \ x_n \in X_n \}$$

At least intuitively, this construction can be identified with $(X_1 \times \ldots \times X_{n-1}) \times X_n$. We shall not attempt to make this precise here because one can easily do so using the discussion below for general Cartesian products.

Infinite products. For the most common mathematical applications, finite products suffice. However, for some purposes — in particular, many graduate courses in mathematics — it is necessary to define the general Cartesian product over an arbitrary (possibly infinite) collection of sets. Typical examples of this sort arise in the study of infinite sequences.

Definition. Let I be an arbitrary index set, and let $\{X_i \mid i \in I\}$ be a collection of sets indexed by I. The ***general Cartesian product*** of the indexed family $\{X_i \mid i \in I\}$ is denoted by symbolism such as

$$\prod \{X_i \mid i \in I\} \quad \text{or} \quad \prod_{i \in I} X_i$$

and is formally specified as follows:

$$\prod_{i \in I} X_i = \{f : I \to \bigcup_{i \in I} X_i \mid (\forall i)(f(i) \in X_i)\}$$

In other words, the general product is the set of all functions defined on the index set I such that the value of the function at a particular index **i** is an element of X_i. Since functions are determined by their values at the points of their domains, it follows that the element **f** in the general Cartesian product is completely determined by the indexed

family of elements $f(i) \in X_i$. In a sense to be made precise later in this section, these elements $x_i = f(i)$ generalize the coordinates of an ordered pair (x, y) in the usual Cartesian product of two sets.

We have already noted that the collection of functions from one set to another is always a set, and this yields the corresponding result for general Cartesian products.

Proposition 1. *Let* I *be an arbitrary index set, and let* $\{X_i \mid i \in I\}$ *be a family of sets indexed by* I. *Then the general Cartesian product of the indexed family* $\{X_i \mid i \in I\}$ *is also a set.*

Proof. As noted in the paragraph preceding the statement of the proposition, the collection of all functions from the set I to the union $X = \cup \{X_i \mid i \in I\}$ is a set. By definition, the general Cartesian product is contained in this set, and therefore it is also a set.■

An n – tuple can be viewed as a function on $\{1, 2, \ldots, n\}$ that takes its value at i to be the i^{th} element of the n – tuple. Therefore, when I is $\{1, 2, \ldots, n\}$ the general definition coincides with the definition for the finite case.

One particular and familiar infinite case arises when the index set is the set $\mathbb{N}$ of natural numbers; this is just the set of all infinite sequences with the i^{th} term in its corresponding set X_i. An even more specialized case occurs when all the factors X_i involved in the product are the same, in which case the construction has an interpretation as "Cartesian exponentiation." Then the big union in the definition is just the set itself, and the other condition is trivially satisfied, so this is just the set of ***all*** functions from I to X, which is the object we have previously called X^I.

In the ordinary Cartesian product of two sets, an element is completely specified by its coordinates, and the same is true for our general definition.

Proposition 2. *Let* I *be an arbitrary index set, and let* $\{X_i \mid i \in I\}$ *be a collection of sets indexed by* I, *and let* x *and* y *be elements of the Cartesian product of the indexed family* $\{X_i \mid i \in I\}$. *Then* $x = y$ *if and only if* $x_i = y_i$ *for all* i.

This follows immediately from the definition of the elements of the Cartesian product as functions defined on the indexing set.■

Formal characterizations of large products

For many purposes it is more convenient to look at large Cartesian products in terms of their functional behavior rather than their set – theoretic construction. In effect, this amounts to giving an axiomatic characterization of such products; from this viewpoint the main point of the previous construction is that it establishes the existence of an object which satisfies the axioms.

Definition. Let $\{X_j\}$ be an indexed family of sets with indexing set J. An ***abstract direct product*** of the indexed family $\{X_j\}$ is pair $(P, \{p_j\})$, where P is a set and $\{p_j\}$ is an indexed family of functions from $p_j : P \rightarrow X_j$ such that the following ***Universal Mapping Property*** holds:

[UMP] *Given an arbitrary set* $\mathbf{Y}$ *and functions* $\mathbf{f_j : Y \to X_j}$ *for each* $\mathbf{j}$**,** *there is a* ***unique*** *function* $\mathbf{f : Y \to P}$ *such that* $\mathbf{p_j \circ f = f_j}$ *for each* $\mathbf{j}$**.**

Footnote. Such characterizations of mathematical constructions by universal mapping properties are fundamental to a topic in the foundations of mathematics known as ***category theory***, which was developed by S. Eilenberg (1913 – 1998) and S. MacLane (1909 – 2005). This subject may be described as an abstract study of functions in mathematics, and among other things it can be used as alternative to set theory for constructing the logical foundations of mathematics (compare the comments at the beginning of Section **IV.3**). We shall not formally discuss the history, motivations and applications of category theory in these notes, but we shall give some online references for such topics. The first reference is a general discussion, the next few give some information about R. Carnap (1891 – 1970), a philosopher whose term ***functor*** was adopted to describe a fundamental concept of category theory, and the final reference is a summary of the main ideas from a slightly more advanced viewpoint.

http://plato.stanford.edu/entries/category-theory/

http://www.iep.utm.edu/c/carnap.htm

http://en.wikipedia.org/wiki/Rudolf_Carnap

http://www.rbjones.com/rbjpub/philos/history/rcp000.htm

http://math.ucr.edu/~res/math205A/categories.pdf

Universal mapping properties like **[UMP]** generally turn out to characterize mathematical constructions uniquely up to a suitably defined notion of equivalence. For our abstract definition of direct products, here is a formal statement of the appropriate uniqueness result.

Theorem 3. (Uniqueness of Direct Products). *Let* $\mathbf{\{X_j\}}$ *be an indexed family of sets with indexing set* $\mathbf{J}$**,** *and suppose that* $\mathbf{(P, \{p_j\})}$ *and* $\mathbf{(Q, \{q_j\})}$ *are direct products of the indexed family* $\mathbf{\{X_j\}}$**.** *Then there is a* ***unique*** $\mathbf{1 - 1}$ *correspondence* $\mathbf{h : Q \to P}$ *such that* $\mathbf{p_j \circ h = q_j}$ *for all* $\mathbf{j}$**.**

Proof. **(**)** First of all, we claim that a function $\mathbf{T : P \to P}$ is the identity if and only if $\mathbf{p_j \circ T = p_j}$ for all $\mathbf{j}$, and likewise $\mathbf{S : Q \to Q}$ the the identity if and only if $\mathbf{q_j S = q_j}$ for all $\mathbf{j}$. These are immediate consequences of the Universal Mapping Property, for in the first case we have $\mathbf{p_j \circ 1_X = p_j}$ for all $\mathbf{j}$, and in the second we have the corresponding equations $\mathbf{q_j \circ 1_Y = q_j}$ for all $\mathbf{j}$.

Since $\mathbf{(P, \{p_j\})}$ is a direct product, the Universal Mapping Property implies there is a unique function $\mathbf{h : Q \to P}$ such that $\mathbf{p_j \circ h = q_j}$ for all $\mathbf{j}$, and likewise since $\mathbf{(Q, \{q_j\})}$ is a direct product, there also exists a unique function $\mathbf{k : P \to Q}$ such that $\mathbf{q_j \circ k = p_j}$ for all $\mathbf{j}$. We claim that $\mathbf{h}$ and $\mathbf{k}$ are inverse to each other; this is equivalent to the pair of identities $\mathbf{h \circ k = 1_Q}$ and $\mathbf{k \circ h = 1_P}$.

To verify these identities, first note that for all $\mathbf{j}$ we have

$$\mathbf{p_j \circ 1_X = p_j = q_j \circ k = p_j \circ h \circ k}$$

for all $\mathbf{j}$ and similarly

$$\mathbf{q_j \circ 1_Y = q_j = p_j \circ h = q_j \circ k \circ h}$$

for all **j**. By the observations in the first paragraph of the proof, it follows that $\mathbf{kh} = \mathbf{1_P}$ and $\mathbf{h} \circ \mathbf{k} = \mathbf{1_Q}$.■

We now need to show that the axiomatic description of direct products is valid for the product construction described above. However, before doing so we verify that the ordinary Cartesian product of two sets also satisfies this property.

Proposition 4. *If* **A** *and* **B** *are sets and* $\mathbf{p_A}$ *and* $\mathbf{p_B}$ *denote the standard coordinate projections from* $\mathbf{A \times B}$ *to* **A** *and* **B** respectively*, then* $\mathbf{(A \times B;\ p_A, p_B)}$ *is a direct product in the sense described above.*

Proof. We need to verify the Universal Mapping Property. Suppose that $\mathbf{f : C \to A}$ and $\mathbf{g : C \to B}$ are functions. Then we may define a function $\mathbf{H : C \to A \times B}$ by the formula $\mathbf{H(c) = (f(c), g(c))}$, and by construction this function satisfies $\mathbf{p_A \circ H = f}$ and $\mathbf{p_B \circ H = g}$. To conclude the proof we need to prove there is a unique function of this type, so assume that $\mathbf{K : C \to A \times B}$ also satisfies $\mathbf{p_A K = f}$ and $\mathbf{p_B K = g}$. Now write $\mathbf{K(c) = (a, b)}$, and note that $\mathbf{a = p_A \circ K(c) = f(c)}$ and $\mathbf{b = p_B \circ K(c) = g(c)}$. Thus we have $\mathbf{K(c) = (f(c), g(c)) = H(c)}$. Since **c** was arbitrary it follows that $\mathbf{H = K}$.■

Theorem 5. *Let* $\{ \mathbf{X_j} \}$ *be an indexed family of sets with indexing set* **J**, *let*

$$\mathbf{\Pi \{ X_j \mid j \in J \} = \Pi_{i \in J} X_j}$$

be the generalized Cartesian product defined above, and for each $\mathbf{k \in J}$ *let*

$$\mathbf{p_k : \Pi \{ X_j \mid j \in J \} \to X_k}$$

be the coordinate projection map such that $\mathbf{p_k(f) = f(k)}$ *for all* **k**. *Then the system*

$$\mathbf{\left(\Pi_{i \in J} X_j, \{ p_j \} \right)}$$

Is a direct product of the indexed family $\mathbf{\{X_j\}}$.

The following "associativity property" of the ordinary Cartesian product will be useful in the proof of the theorem.

Lemma 6. Let **A, B** *and* **C** *be sets. Then there is a canonical* $\mathbf{1 - 1}$ *correspondence* **T** *from* $\mathbf{(A \times B) \times C}$ *to* $\mathbf{A \times (B \times C)}$ *defined by the formula*

$$\mathbf{T((a, b), c) = (a, (b, c))}$$

for all $\mathbf{a \in A}$, $\mathbf{b \in B}$, *and* $\mathbf{c \in C}$.

***Proof of Lemma* 6. (**)** The formula for **T** is given in the lemma; we need to show this map is $\mathbf{1 - 1}$ and onto. To see that it is $\mathbf{1 - 1}$, suppose that

$$\mathbf{T((a, b), c) = T((x, y), z).}$$

By construction this means that $\mathbf{(a, (b, c)) = (x, (y, z))}$. Since ordered pairs are equal if and only if their respective coordinates are equal, it follows that we have $\mathbf{a = x}$ and $\mathbf{(b, c) = (y, z)}$. The second equation then implies $\mathbf{b = y}$ and $\mathbf{c = z}$, and from these we conclude that $\mathbf{((a, b), c) = ((x, y), z)}$. Therefore the mapping **T** is $\mathbf{1 - 1}$. To see that it is onto, note that every element of the codomain has the form $\mathbf{((a, b), c)}$

for suitable choices of **a, b** and **c,** and by the definition of **T** each such element belongs to the image of **T.**■

***Proof of Theorem* 5. (***)** All we need to do is verify the Universal Mapping Property. Suppose that we are given functions $f_j : Y \to X_j$ for each **j.**

For each **j** let G_j denote the subset of all **(j, y, x)** in $\{ j \} \times (Y \times X_j)$ such that **(y, x)** lies in the graph of f_j. Denote the union $\cup_j X_j$ of all the sets X_j by **X,** and let $G \subset J \times (Y \times X)$ be the union $\cup_j G_j$. Let $G' \subset (J \times Y) \times X$ denote the image of the set **G** under the associativity map in the lemma. **CLAIM:** For each **(j, y)** there is a unique **x** such that the object **(** (**j, y**)**, x)** belongs to **G′.** This follows immediately from the fact that each f_j is a function.

Consider now the $1 - 1$ correspondence

$$J \times (Y \times X) \to J \times (X \times Y) \to (J \times X) \times Y \to Y \times (J \times X)$$

which takes **((j, y) , x)** to **((y, j) , x).** The middle step of this map is the associativity map in the lemma, and the outside steps merely transpose the coordinates in the appropriate ordered pairs. Let G^* denote the image of **G** under this mapping, and for each y in Y let G_y^* denote the intersection of G^* with the set $\{y\} \times (J \times X)$. By the final two sentences of the preceding paragraph, it follows that G_y^* is the graph of a function H_y from **J** to **X,** and in fact the assumption on the functions f_j imply that H_y is the graph of a function such that $H_y(j)$ belongs to f_j for each **j.** The definition of the general Cartesian product then implies that H_y defines an element of the product $\prod\{X_j \mid j \in J\}$. By construction we have $H_y(j) = f_j(y)$, and this verifies the projection identities for the function we have constructed, proving the existence of a function from **Y** into the general Cartesian product with the required properties.

We now need to prove uniqueness. Suppose that **H** and **K** are functions from **Y** into the product which satisfy the basic projection identities. The latter imply that $H_y(j) = f_j(y)$ and $K_y(j) = f_j(y)$ for all **j** and **y.** But the latter equations mean that **H** and **K** define the same functions from **J** to **X** for each **y,** so that $H_y = K_y$ for all **y,** which in turn implies that **H = K.**■

Technical note. Our definition of function differs from that of Halmos (we are including the codomain as part of the structure). Because of this, the first sentence in the exercise on page 37 of Halmos must be modified to as follows in order to match our formulation: Instead of saying that the sets in question are equal, we need to say that there is a $1 - 1$ correspondence between them. More precisely, if **J** is an index set, with $\{X_j \mid j \in J\}$ a collection of sets indexed by **J** and for each $j \in J$ we are given a subset A_j of X_j, then according to Halmos' definition we know that

$$\prod \{A_j \mid j \in J\} \quad \textit{is a subset of} \quad \prod \{X_j \mid j \in J\}$$

but in our formulation one only has the following weaker statement, which is entirely adequate for all practical purposes:

Proposition 7. *In the setting above, let* e_j *denote the inclusion mapping from* A_j *to* X_I. *Then there is a* ***unique canonical*** **1 – 1** ***mapping***

$$\mathbf{e} : \prod \{ A_j \mid j \in J \} \rightarrow \prod \{ X_j \mid j \in J \}$$

such that for each element **a** *of the domain and each indexing variable* **j** *we have the coordinate identity* $\mathbf{e(a)_j = e_j(a_j)}$.

This mapping is often denoted by $\prod \{ e_j \mid j \in J \}$ or more simply by $\prod e_j$.

Using the map **e** we may naturally identify the domain with the elements of the codomain such that for each **j,** the j^{th} coordinate lies in A_j.

Proof. **(∗)** Usually the fastest way of proving such a result is to apply the Universal Mapping Property**,** and doing so will also give us an opportunity to illustrate how the latter is used in mathematical work**.**

Let $\{ p_j \}$ denote the family of coordinate projection maps for $\prod \{ X_j \mid j \in J \}$**,** and similarly let $\{ q_j \}$ denote the corresponding coordinate projection maps for the other product $\prod \{ A_j \mid j \in J \}$**.** For each indexing variable **k,** define a mapping

$$f_k : \prod \{ A_j \mid j \in J \} \rightarrow X_k$$

by setting f_k equal to the composite $e_k \circ q_k$**.** The Universal Mapping Property then implies the existence of a unique function

$$\mathbf{e} : \prod \{ A_j \mid j \in J \} \rightarrow \prod \{ X_j \mid j \in J \}$$

such that for each $j \in J$ we have $p_j \circ e = e_j \circ q_j$**.** This is equivalent to the condition on coordinates, so all that remains is to verify that **e** is a $1-1$ mapping**.** Since elements of a Cartesian product are determined by their coordinates, the latter reduces to showing that if **e(x) = e(y),** then for each $j \in J$ we have $x_j = y_j$**.** Let **J** be fixed but arbitrary, and consider the following string of equations which follows from **e(x) = e(y):**

$$e_j(x_j) = e(x)_j = e(y)_j = e_j(y_j)$$

Since the inclusion map e_j is $1-1$ by construction, it follows that $x_j = y_j$**.** Since **j** was arbitrary, this means that all the corresponding coordinates of **x** and **y** are equal and consequently that **x = y,** proving that **e** is also a $1-1$ mapping**.**■

Applications of the Universal Mapping Property

We shall conclude this section with a few examples illustrating the use of the Universal Mapping Property for products to answer some basic questions**.** We shall begin with a version of the recursive property for finite Cartesian products mentioned at the beginning of this section**.**

Proposition 8. *Let* **A, B, C** *be sets. Denote the projections from* $(A \times B) \times C$ *to* $A \times B$ *and* **C** *by* $p_{1,2}$ *and* p_3 *respectively, and for* $i = 1$ *or* **2** *let* p_i *denote the projection of* $A \times B$ *to* **A** *and* **B** *respectively. Define maps* q_i *by* $q_i = p_i \circ p_{1,2}$ *for* $i = 1$ *or* **2,** *and* $q_3 = p_3$**.** *Then the system* $\big((A \times B) \times C, \{q_1, q_2, q_3\} \big)$ *satisfies the Universal Mapping Property for products.*

Proof. Suppose that $f_1 : D \rightarrow A$, $f_2 : D \rightarrow B$, $f_3 : D \rightarrow C$ are functions. By the Universal Mapping Property for twofold products there is a unique function $f_{1,2} : D \rightarrow A \times B$ such

that $p_i \circ f_{1,2} = f_i$ for $i = 1, 2$. Similarly, there is a unique function $f : D \to (A \times B) \times C$ such that $p_{1,2} \circ f = f_{1,2}$ and $p_3 \circ f = f_3$. Since $q_3 = p_3$, clearly $q_3 \circ f = f_3$. Furthermore, if $i = 1, 2$ then $q_i \circ f = p_i \circ p_{1,2} \circ f = p_i \circ f_{1,2} = f_i$, proving the existence part of the Universal Mapping Property.

To prove uniqueness, suppose that the projections of $h, k : B \to (A \times B) \times C$ onto the sets A, B, C are equal to the mappings f_i. We first claim that the projections of h and k onto $A \times B$ are equal. The projections of h and k onto $A \times B$ satisfy $q_i \circ h = f_i = q_i \circ k$ for $i = 1$ or 2, and thus by the Universal Mapping Property for twofold products it follows that $p_{1,2} \circ h = p_{1,2} \circ k$.

By assumption we also have $q_3 \circ h = f_3 = q_3 \circ k$, and hence by the Universal Mapping Property for the twofold product $(A \times B) \times C$ it follows that $h = k$.■

Here is another example, which is also a good illustration of proving that a mapping is bijective.

Proposition 9. *Let* A, B, C *be sets.*

(1) *There is a unique mapping* T *from* $(A \times B) \times C$ *to* $(C \times A) \times B$ *such that* $T(x, y, z) = (z, x, y)$ *for all* x, y, z.

(2) *The mapping* T *is bijective, and if* $A = B = C$ *the inverse is given by* $T \circ T$.

Proof. By the Universal Mapping Property for products there is a unique mapping T from $(A \times B) \times C$ to $(C \times A) \times B$ such that $p_1 \circ T = p_3$, $p_2 \circ T = p_1$, and $p_3 \circ T = p_2$. By construction, such a map satisfies $T(x, y, z) = (z, x, y)$ for all x, y, z.

We first show that T is injective. If $T(x, y, z) = T(x', y', z')$, then by definition of T we have $(z, x, y) = (z', x', y')$ and the latter implies $x = x'$, $y = y'$, and $z = z'$. Next we prove that T is surjective. To solve the equation $T(x, y, z) = (u, v, w)$ we need to find (x, y, z) so that $(z, x, y) = (u, v, w)$. Clearly $x = v$, $y = w$, $z = u$ gives a solution, so that map is surjective as claimed.

If we have $A = B = C$ then $T^{-1}(u, v, w) = (x, y, z)$ implies $(z, x, y) = (u, v, w)$, so that $T^{-1}(u, v, w) = (v, w, u)$. But the latter is equal to $T(w, u, v) = T \circ T(u, v, w)$, and therefore $T^{-1} = T \circ T$ as required.■

V.3 : Transfinite cardinal numbers

(Halmos, §§ 22 – 23; Lipschutz, §§ 6.1 – 6.3, 6.5)

Early in his work on infinite sets, Cantor considered the problem of comparing the relative sizes of such sets. Specifically, given two infinite sets, the goal is to determine if one has the same size as the other or if there are different orders of infinity such that one set is of a lower order than the other. Many of Cantor's results were entirely unanticipated, and ultimately his findings led mathematicians to make major changes to their perspectives on infinite objects. In several respects the material in this section is the central part of these notes.

Definition. If **A** and **B** are sets, we write $|A| = |B|$, and say that *the cardinality of* **A** *is equal to the cardinality of* **B** (or they have the same cardinality, *etc.*) if there is a $1-1$ onto mapping $f : A \to B$.

The relationship $|A| = |B|$ is clearly reflexive because the identity on **A** is a $1-1$ onto map from **A** to itself, and if $|A| = |B|$, then $|B| = |A|$ is also true because the inverse of **f** is a $1-1$ onto mapping from **B** to **A.** Finally, if $|A| = |B|$ and $|B| = |C|$, then we also have $|A| = |C|$, for if we have $1-1$ onto mappings $f : A \to B$ and $g : B \to C$, then the composite $g \circ f$ is a $1-1$ onto mapping from **A** to **C.** In particular, if **X** is a set and we define a binary relation of "having the same cardinality" on **P(X)** to mean that $|A| = |B|$, then having the same cardinality defines an equivalence relation on **P(X).** In such a setting, the ***cardinal number*** of a subset **A** may be interpreted as the equivalence class of all sets **B** which have the same cardinality as **A.** This relation is actually independent of the choice of set **X** containing **A** and **B,** for if **Y c**ontains **X** then **A** and **B** determine the same equivalence class in **P(X)** if and only if they determine the same equivalence class in **P(Y).**

The restriction to subsets of a given set is awkward, but some restrictive condition is needed and we have chosen one that is relatively simple to state. Initially, many mathematicians and logicians including Cantor, B. Russell and G. Frege (1848 – 1925), attempted to define the cardinal number of a set **X** as the equivalence class of all sets **Y** that can be put into a $1-1$ correspondence with **X,** but a definition of this type cannot be made logically rigorous because the family of all such objects is "too large" to be a set.

Finite and infinite sets

For finite sets, the notion of cardinality has been understood for thousands of years.

Definition. If **n** is a positive integer, then a nonempty set **X** has ***cardinal number equal to*** **n** if there is a $1-1$ correspondence between **X** and $\{0, \ldots, n-1\}$. By the results of Section V.3, it follows that there is at most one **n** such that a set has cardinal number equal to **n.** The definition is extended to nonnegative integers by taking the cardinality of the empty set to be 0. We say that a set **X** is ***finite*** if it has cardinal number equal to **n** for some **n** and that **X** is ***infinite*** otherwise.

Cantor's important — and in fact revolutionary — insight was that one can define ***transfinite cardinal numbers*** to measure the relative sizes of infinite sets.

Partial ordering of cardinalities

Definition. If **A** and **B** are sets, we write $|A| \leq |B|$, and say that *the cardinality of* **A** *is less than or equal to the cardinality of* **B** if there is a $1-1$ map from **A** to **B.**

The notation suggests that this relationship should behave like a partial ordering (in analogy with finite sets we would like it to be a linear ordering, but reasons for being more modest in the infinite case will be discussed later). It follows immediately that the relation we have defined is ***reflexive*** (take the identity map on a set **A**) and ***transitive***

(given $\mathbf{1-1}$ maps $\mathbf{f: A \to B}$ and $\mathbf{g: B \to C}$, the composite $\mathbf{g \circ f}$ is also $\mathbf{1-1}$), but the proof that it is ***antisymmetric*** is decidedly nontrivial:

Theorem 1. (Schröder – Bernstein Theorem.) *If* **A** *and* **B** *are sets such that there are* $\mathbf{1-1}$ *maps* $\mathbf{A \to B}$ *and* $\mathbf{B \to A}$, *then* $\mathbf{|A| = |B|}$.

Proof. **(**)** We shall give the classic argument from the (third edition of the) book by G. [= Garrett] Birkhoff (1911 – 1996) and S. MacLane (1909 – 2005) cited below; the precise reference is page 340.

> G. Birkhoff and S. MacLane, ***A Survey of Modern Algebra.*** (Reprint of the Third 1968 Edition). Chelsea Publishing, New York, NY, 1988. ISBN: 0 – 023 – 74310 – 7.

Let $\mathbf{f: A \to B}$ and $\mathbf{g: B \to A}$ be the $\mathbf{1-1}$ mappings which exist by the assumptions. Each $\mathbf{a \in A}$ is the image of at most one parent element $\mathbf{b \in B}$ such that $\mathbf{a = g(b)}$; in turn, the element **b** (if it exists) has at most one parent element in **A**, and so on. The idea is to trace back the ancestry of each element as far as possible. For each point in **A** or **B** there are exactly three possibilities:

1. The ancestral chain may go back forever.
2. The ancestral chain may end in **A**.
3. The ancestral chain may end in **B**.

We can then split **A** and **B** into three pairwise disjoint pieces corresponding to these cases, and we shall call the pieces $\mathbf{A_1, A_2, A_3}$ and $\mathbf{B_1, B_2, B_3}$ (where the possibilities are ordered as in the list).

The map **f** defines a $\mathbf{1-1}$ correspondence between $\mathbf{A_1}$ and $\mathbf{B_1}$ (and likewise for **g**). Furthermore, **g** defines a $\mathbf{1-1}$ correspondence from $\mathbf{B_2}$ to $\mathbf{A_2}$, and **f** defines a $\mathbf{1-1}$ correspondence from $\mathbf{A_3}$ to $\mathbf{B_3}$. If we combine these $\mathbf{1-1}$ correspondences $\mathbf{A_1 \leftrightarrow B_1}$, $\mathbf{A_2 \leftrightarrow B_2}$, and $\mathbf{A_3 \leftrightarrow B_3}$, we get a $\mathbf{1-1}$ correspondence between all of **A** and all of **B**.■

Here is an immediate consequence of the Schröder – Bernstein Theorem:

Proposition 2. *If* **A** *is an infinite subset of the nonnegative integers* $\mathbb{N}$, *then* $\mathbf{|A| = |\mathbb{N}|}$.

Proof. **(*)** We shall define a $\mathbf{1-1}$ mapping from $\mathbb{N}$ to **A** recursively; the existence of such a map will imply $\mathbf{|A| \leq |\mathbb{N}|}$. Since **A** is a subset of $\mathbb{N}$ we also have the reverse inequality $\mathbf{|\mathbb{N}| \leq |A|}$, and therefore $\mathbf{|A| = |\mathbb{N}|}$ by the Schröder – Bernstein Theorem.

Since $\mathbb{N}$ is well – ordered, it follows that every nonempty subset of **A** has a least element. Define **f** recursively by setting $\mathbf{f(0)}$ equal to the least element of **A**, and if we are given a partial $\mathbf{1-1}$ function $\mathbf{g_n: \{0, \ldots, n-1\} \to A}$, extend the definition to the set $\mathbf{\{0, \ldots, n\}}$ by noting that the image of $\mathbf{g_n}$ is a proper subset of **A** (which is infinite) and taking $\mathbf{g_{n+1}(n)}$ to be the ***first*** element in $\mathbf{A - \mathit{Image}(g_n)}$. The increasing union of these functions will be the required function from $\mathbb{N}$ to **A**. It is $\mathbf{1-1}$ because it is $\mathbf{1-1}$ on each subset $\mathbf{\{0, \ldots, n-1\}}$; if $\mathbf{f(x) = f(y)}$, then there is some **n** such that **x** and **y** both belong to $\mathbf{\{0, \ldots, n-1\}}$, and therefore it follows that **x** and **y** must be equal.■

Definition. A set is ***countable*** if it is in $\mathbf{1-1}$ correspondence with a subset of the natural numbers, and it is ***denumerable*** if it is in $\mathbf{1-1}$ correspondence with the natural numbers. However, many writers also use countable as a synonym for denumerable, so one must be careful. Frequently one also sees the phrase ***"countably infinite"*** employed as a synonym for denumerable.

Following Cantor, it is customary to denote the cardinal number of the natural numbers by $\aleph_0$ (verbalized as ***aleph – null***).

The next result generalizes a simple fact about cardinal numbers from finite sets to countable sets.

Proposition 3. *Suppose that* **A** *is a nonempty countable set and there is a surjective mapping* **f** *from* **A** *to* **B.** *Then* **B** *is also countable, and in fact* $|\mathbf{B}| \leq |\mathbf{A}|$.

Proof. By hypothesis there is a $\mathbf{1-1}$ correspondence between **A** and a subset of the nonnegative integers $\mathbb{N}$, and thus one can use the standard ordering of the latter to make **A** into a well – ordered set. Define a function $\mathbf{h : B \to A}$ as follows: Given a typical element $\mathbf{b \in B}$, take **h(b)** to be the least element in the inverse image $\mathbf{f^{-1}[\{b\}]}$. Then by definition we have $\mathbf{f \circ h(b) = b}$. The result will follow from the Proposition 2 provided we can show that **h** is a $\mathbf{1-1}$ mapping, and this holds because $\mathbf{h(x) = h(y)}$ implies $\mathbf{x = f \circ h(x) = f \circ h(y) = y}$.■

VI.3 : Countable and uncountable sets

(Halmos, §§ 23 – 23; Lipschutz, §§ 6.3 – 6.7)

A theory of transfinite cardinal numbers might not be particularly useful if all infinite sets had the same cardinality. In the first paragraphs of this unit we indicated that the cardinalities of $\mathbb{R}$ and $\mathbb{N}$ are different, and the goal of this section is to prove this result. The first step in this process is to extend some basic arithmetic operations on $\mathbb{N}$ to arbitrary transfinite cardinal numbers.

Binary operations on cardinal numbers

One can perform a limited number of arithmetic operations with cardinal numbers, but it is necessary to realize that these do not enjoy all the familiar properties of the corresponding operations on positive integers. Before doing so, it is convenient to introduce a set – theoretic construction which associates to two sets **A** and **B** a third set which is a union of disjoint isomorphic copies of **A** and **B.** Formally, the ***disjoint sum*** (or ***disjoint union***) is defined to be the set

$$\mathbf{A \coprod B = A \times \{1\} \cup B \times \{2\}}$$

and the standard ***injection*** mappings $i_A : A \to A \amalg B$ and $i_B : B \to A \amalg B$ are defined by

$$i_A(a) = (a, 1) \quad \text{and} \quad i_B(b) = (b, 2)$$

respectively. By construction, we have the following elementary consequences of the definition:

Proposition 1. *Suppose that we are given the setting and constructions described above.*

(1) *The injection maps* i_A *and* i_B *determine* $1 - 1$ *correspondences* j_A *from* A *to* $i_A[A]$ *and* j_B *from* B to $i_B[B]$.

(2) *The images of* A *and* B *are disjoint.*

(3) *The union of the images of* A *and* B *is all of* $A \amalg B$.

The proof of this result is fairly simple, but we shall include it for the sake of completeness and because it is not necessarily easy to locate in the literature.

***Proof of* (1).** The sets $i_A[A]$ and $i_B[B]$ are equal to $A \times \{1\}$ and $B \times \{2\}$ respectively, and we have $j_A(a) = (a, 1)$ and $j_B(b) = (b, 2)$. It follows that inverse maps are given by projection onto A and B respectively.■

***Proof of* (2).** The first coordinate of an element in the image of i_A is equal to **1**, and the first coordinate of an element in the image of i_B is equal to **2**. Therefore points in the image of one map cannot lie in the image of the other.■

***Proof of* (3).** Clearly the union is contained in $A \amalg B$. Conversely, if we are given a point in the latter, then either it has the form $(a, 1) = i_A(a)$ or $(b, 2) = i_B(b)$.■

Definition. (Addition of cardinal numbers). If A and B are sets with cardinal numbers $|A|$ and $|B|$ respectively, then the *sum* $|A| + |B|$ is equal to $|A \amalg B|$.

Definition. (Multiplication of cardinal numbers). If A and B are sets with cardinal numbers $|A|$ and $|B|$ respectively, then the *product* $|A| \times |B| = |A| \cdot |B| = |A|\,|B|$ is equal to $|A \times B|$.

Definition. (Exponentiation of cardinal numbers). If A and B are sets with cardinal numbers $|A|$ and $|B|$ respectively, then the *power operation* $|A|^{|B|}$ is equal to $|A^B|$, where A^B denotes the set of functions from B to A (as in Unit IV).

In order to justify these definitions we need to verify two things; namely, that **[** i **]** these definitions agree with the counting results Section V.3 if A and B are finite sets, and also **[** ii **]** that the construction is ***well – defined***. We have defined the operations by choosing specific sets A and B with given cardinal numbers, and we need to make sure that if choose another pair of sets, say C and D, then we obtain the same cardinal numbers. The first point is easy to check; if A and B are finite sets, then the formulas in Section V.3 show that the numbers of elements in $A \amalg B$, $A \times B$, and A^B are respectively equal to $|A| + |B|$, $|A| \cdot |B|$ and $|A|^{|B|}$. The following elementary result disposes of the second issue.

Proposition 2. *Suppose that we are given sets* **A, B, C, D** *and we also have* $1-1$ *correspondences* $f : A \to C$ *and* $g : B \to D$. *Then there are* $1-1$ *correspondences from* $A \coprod B$, $A \times B$, *and* A^B *to* $C \coprod D$, $C \times D$, *and* C^D *respectively.*

Proof. Define mappings

$$H : A \coprod B \to C \coprod D, \quad J : A \times B \to C \times D, \quad K : A^B \to C^D$$

by the following formulas:

$$H(a, 1) = (f(a), 1), \quad H(b, 2) = (g(b), 2)$$

$$J(a, b) = (f(a), g(b))$$

$$[K(\varphi)](c) = f \circ \varphi \circ g^{-1}(c)$$

Define mappings in the opposite direction(s)

$$L : C \coprod D \to A \coprod B, \quad M : C \times D \to A \times B, \quad N : C^D \to A^B$$

by substituting f^{-1}, g^{-1}, and g for the variables **f, g,** and g^{-1} in the corresponding definitions of **H, J** and **K** respectively. Routine calculations (left to the reader) show that the maps **L, M** and **N** are inverses to the corresponding mappings **H, J** and **K.**■

We shall see that operations on transfinite cardinal numbers do not satisfy some of the fundamental properties that hold for integers; for example, we shall see below that an equation of the form $x + y = x$ does not necessarily imply that $x = 0$. However, here is one important relationship that does generalize:

Proposition 3. *If* **A** *is a set then* $|P(A)| = 2^{|A|}$.

Proof. We need to define a $1-1$ correspondence χ from **P(A)** to the set of functions from **A** to the set $\{0, 1\}$. Given a subset **B,** its ***characteristic function*** $X_B : A \to \{0, 1\}$ is defined by $X_B(x) = 1$ if $x \in B$ and 0 otherwise. The map sending a subset to its characteristic function is $1-1$ because $B = X_B^{-1}[\{1\}]$, so that $X_B = X_C$ implies $B = X_B^{-1}[\{1\}] = X_C^{-1}[\{1\}] = C$. To see this is onto, let $f : A \to \{0, 1\}$ and note that by definition we have $f = X_B$ where $B = f^{-1}[\{1\}]$.■

Finally, we have the following fundamentally important result due to Cantor.

Theorem 4. *If* **A** *is a set then* $|A| < |P(A)| = 2^{|A|}$.

Proof. **(*)** Define a $1-1$ mapping from **A** to **P(A)** sending an element $a \in A$ to the one point subset $\{a\}$. This shows that $|A| \leq |P(A)|$.

The proof that $|A| \neq |P(A)|$ is given by the ***Cantor diagonal process.*** Suppose that there is a $1-1$ correspondence $F : A \to \{0, 1\}^A$. The idea is to construct a new function $g \in \{0, 1\}^A$ that is not in the image of **F**. Specifically, choose **g** such that, for each $a \in A$, the value **g(a)** will be the unique element of $\{0, 1\}$ which is not equal to $[F(a)](a)$; recall that **F(a)** is also a function from **A** to $\{0, 1\}$ and as such it can be evaluated at **a.** Since the values of **g** and **F(a)** at $a \in A$ are different, these two functions are distinct, and since $a \in A$ is arbitrary it follows that **g** cannot lie in the image of **F.**

However, we were assuming that **F** was onto**,** so this yields a contradiction**.** Therefore there cannot be a $\mathbf{1-1}$ correspondence between **A** and **P(A)**.■

Comments on the method of proof. The reason for the name ***diagonal process*** is illustrated below when **A** is the set $\mathbb{N}^+$ of positive integers. One assumes the existence of a $\mathbf{1-1}$ correspondence between $\mathbb{N}^+$ and $\mathbf{P(\mathbb{N}^+)}$ and identifies the latter with the set of functions from $\mathbb{N}^+$ to $\mathbf{\{0, 1\}}$ in the standard fashion**.** Then for each positive integer one has an associated sequence of $\mathbf{0}$**'**s and $\mathbf{1}$**'**s that are indexed by the positive integers**,** and one can represent them in a table or matrix form as illustrated below**,** in which each of the terms $\mathbf{x_j}$ (where **x** is a letter and **j** is a positive integer) is equal to either $\mathbf{0}$ or $\mathbf{1}$**.**

$$
\begin{array}{l}
1 \cdots \mathbf{a_1}.a_2.a_3.a_4.a_5\cdots\ldots \\
2 \cdots b_1.\mathbf{b_2}.b_3.b_4.b_5\cdots\ldots \\
3 \cdots c_1.c_2..\mathbf{c_3}.c_4.c_5\cdots\ldots \\
4 \cdots d_1.d_2.d_3.\mathbf{d_4}.d_5\cdots\ldots \\
5 \cdots e_1.e_2.e_3.e_4.\mathbf{e_5}\cdots\ldots \\
\ldots
\end{array}
$$

The existence of a $\mathbf{1-1}$ correspondence implies that all sequences appear on the list**.** However**,** if we change each of the bold entries (***i.e.***, the entry in the $\mathbf{n^{th}}$ row and $\mathbf{n^{th}}$ column for each **n**) by taking $\mathbf{0}$ if the original entry is $\mathbf{1}$ and vice versa**,** we obtain a new sequence that is not already on the list**,** showing that $\mathbf{P(\mathbb{N}^+)}$ cannot be put into correspondence with $\mathbb{N}^+$ and thus represents a higher order of infinity**.**■

The preceding result implies that ***"there is no set of all cardinal numbers."*** Stated differently**,** there is no set **S** such that every set **A** is in $\mathbf{1-1}$ correspondence with a subset of **S.** If such a set existed, then the set **P(S)** would be in $\mathbf{1-1}$ correspondence with some subset $\mathbf{T \subset S}$**,** and hence we would obtain the contradiction

$$\mathbf{|P(S)| = |T| \leq |S| < |P(S)|.}\blacksquare$$

This observation is often called ***Cantor's Paradox***, and was noted by Cantor in 1899**;** it is very close to the original set – theoretic paradox that was discovered by C. Burali – Forti (1861 – 1931) a few years earlier and will be discussed in the next section.

Some basic rules of cardinal arithmetic

Addition and multiplication of cardinal numbers satisfy many of the same basic equations and inequalities that hold for nonnegative integers. Here is a list of the most fundamental examples**:**

Theorem 5. *The sum and product operations on cardinal numbers have the following properties for all cardinal numbers* α**,** β *and* γ**:**

(Associative law of addition) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$

(Commutative law of addition) $\alpha + \beta = \beta + \alpha$

(Associative law of multiplication) $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$

(Commutative law of multiplication) $\alpha \cdot \beta = \beta \cdot \alpha$

(Distributive law) $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$

(Equals added to unequals) $\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$

(Equals multiplied by unequals) $\alpha \leq \beta \Rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma$

The verifications of all these equations and inequalities are extremely straightforward. For example, the commutative law of addition merely reflects the commutative law for set – theoretic unions, and the commutative law of multiplication reflects the existence of the canonical $1 - 1$ correspondence from the Cartesian product $A \times B$ to the analogous product with interchanged factors $B \times A$, which sends **(a, b)** to **(b, a).** All the details are worked out on page 161 of Lipschutz. These proofs do not use our formal definition for the sum of two cardinal numbers, but instead they use the following characterization:

Lemma 6. *If* **X** *and* **Y** *are disjoint sets, then* $|X \cup Y| = |X| + |Y|$. *Furthermore, if* **A** *and* **B** *are arbitrary sets, then there exist sets* **X** *and* **Y** *such that* $|X| = |A|$, $|Y| = |B|$, *and also* $X \cap Y = \emptyset$.

Proof. The second part of the lemma follows from our disjoint union construction. The first part will follow if there is a $1 - 1$ correspondence **H** from $X \amalg Y$ to $X \cup Y$. An explicit construction of such a map is given by $H(x, 1) = x$ and $H(y, 2) = y$. Since the image of this map contains both **X** and **Y,** it follows that **H** is onto. To see it is $1 - 1$, note that the restrictions to $X \times \{1\}$ and $Y \times \{2\}$ are both $1 - 1$ so the only way the map might not be $1 - 1$ is if one has $x \in X$ and $y \in Y$ such that $H(x, 1) = H(y, 2)$. The latter would imply that **X** and **Y** are not disjoint, and since we know they are disjoint it follows that there are no such elements **x** and **y,** so that **H** must also be $1 - 1$ as required.■

Although arbitrary cardinal numbers satisfy many of the same basic equations and inequalities as nonnegative integers, it is important to recognize that some algebraic properties of the latter do not extend. In particular, the results below prove that a cardinal number equation of the form $\alpha + \beta = \alpha$ does ***not*** necessarily imply $\beta = 0$. Similarly, an equation of the form $\alpha \cdot \beta = \alpha$ does ***not*** necessarily imply that either $\beta = 1$ or $\alpha = 0$.

Identities and inequalities for cardinal numbers

The following simple result illustrates a major difference between finite and transfinite cardinals:

Proposition 7. *If* **A** *is finite, then* $|A| + \aleph_0 = \aleph_0$.

Proof. If $|A| = 0$ this is trivial. Suppose now that $|A| = 1$, and let **a** be the unique element of **A.** Let $\mathbb{N}$ be the natural numbers, and define a mapping **h** from $A \amalg \mathbb{N}$ to $\mathbb{N}$ by setting $h(a, 1) = 0$ and $h(n, 2) = n + 1$ for $n \in \mathbb{N}$. By the Peano Axioms for the natural numbers, the restriction of **h** to $\mathbb{N} \times \{2\}$ is injective, and its image is the set of all

positive integers. Since **h(a, 1) = 0,** it follows that **h** is $1-1$ and onto. Therefore we have $1 + \aleph_0 = \aleph_0$.

From this point on we proceed by induction on **k = |A|.** Suppose we know the result in this case; we need to prove it is also true for **|A| = k + 1.** This is an direct consequence of the following chain of equations:

$$(k + 1) + \aleph_0 = (1 + k) + \aleph_0 = 1 + (k + \aleph_0) = 1 + \aleph_0 = \aleph_0$$

This completes the proof of the inductive step and hence of the result itself.■

The following standard identities involving $\aleph_0$ were first noted by Galileo (thus is frequently known as ***Galileo's Paradox***) and Cantor respectively.

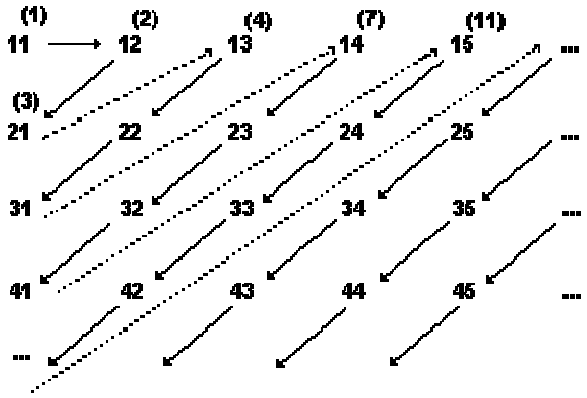
Theorem 8. (Idempotent Laws). *We have* $\aleph_0 + \aleph_0 = \aleph_0$ *and* $\aleph_0 \cdot \aleph_0 = \aleph_0$.

Proof. Let $\mathbb{N}$ be the nonnegative integers, and let $\mathbf{N(0)}$ and $\mathbf{N(1)}$ denote the subsets of even and odd nonnegative integers respectively. Then the mappings sending **n** to **2n** and **2n + 1** define $1-1$ correspondences from $\mathbb{N}$ to **N(0)** and **N(1)** respectively. Since $\mathbf{N(0)} \cup \mathbf{N(1)} = \mathbb{N}$ and $\mathbf{N(0)} \cap \mathbf{N(1)} = \emptyset$, it follows that

$$\aleph_0 = |\mathbb{N}| = |\mathbf{N(0)}| + |\mathbf{N(1)}| = |\mathbb{N}| + |\mathbb{N}| = \aleph_0 + \aleph_0$$

proving the first assertion in the theorem.

To prove the second assertion, we shall first define a $1-1$ mapping from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ by defining an equivalent map from $\mathbb{N}^+ \times \mathbb{N}^+$ to $\mathbb{N}^+$ by a diagonal construction due to Cantor (also see Halmos, page 92). The following picture illustrates the idea behind the function's definition; the explicit formula is **f(m, n) = ½(m + n – 1)(m + n – 2) + m.**



(***Source:*** http://www.cut-the-knot.org/do_you_know/numbers.shtml)

A verification that **f** is $1-1$ is sketched in the exercises. We also have an easily defined $1-1$ mapping in the opposite direction sending **n** to **(n, 0).** We can now use the Schröder – Bernstein Theorem to prove the equality $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$, or equivalently that $\aleph_0 \cdot \aleph_0 = \aleph_0$.■

Corollary 9. *For each positive integer* **n** *we have* $n \cdot \aleph_0 = \aleph_0$ *and* $(\aleph_0)^n = \aleph_0$.

Proof. The main result proves the result for $n = 2$, and it is trivial if $n = 1$.

The proof that the special case $n = 2$ implies the general case can be done abstractly as follows: Suppose that we are given any associative binary operation and an element a such that $a^2 = a$. Under this condition we claim that $a^n = a$ for all $n > 1$. The case $n = 2$ is given, so assume that the result is true for some $k > 1$. Then we have

$$a^{k+1} = a^k a = aa = a$$

completing the inductive step of the derivation. We have written the binary operation multiplicatively, but of course we also could have written it additively, and thus the whole argument works for both addition and multiplication of cardinal numbers.■

We now have the following standard consequences.

Proposition 10. *Let* $\mathbf{C}$ *be a countable family of sets, each of which is countable. Then the countable union of the countable sets* $\$(\mathbf{C}) = \cup_{B \in C} B$ *is also countable.*

Proof. Let A be the set of all ordered pairs (x, B) such that $x \in B$ and $B \in \mathbf{C}$. If we define $g : A \to \$(\mathbf{C})$ by projection onto the first coordinate, then g is onto. By Proposition 3, it will suffice to prove that A is countable. Let $f : \mathbf{C} \to \mathbb{N}$ be a $1 - 1$ mapping, and for each $B \in \mathbf{C}$ define a $1 - 1$ mapping $g_B : B \to \mathbb{N}$. All these maps exist because $\mathbf{C}$ is countable and each subset B in $\mathbf{C}$ is countable. Next, define a mapping $h: A \to \mathbb{N} \times \mathbb{N}$ by $h(x, B) = (g_B(x), f(B))$. We claim that h is $1 - 1$. Suppose that we have $h(x, B) = h(y, D)$. By definition we then have $f(B) = f(D)$, and since f is $1 - 1$ it follows that $B = D$. Once again using the definitions we see that $g_B(x) = g_B(y)$, and since g_B is $1 - 1$ it follows that $x = y$. This completes the proof that h is $1 - 1$, which implies the key assertion that A is countable; as noted earlier in the discussion, this completes the proof.■

Proposition 11. *If* $\mathbb{Z}$ *and* $\mathbb{Q}$ *are the integers and rational numbers respectively, then we have* $|\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$.

The result for the integers was anticipated in Galileo's writings on infinite sets, but the result regarding the rational numbers was something of a surprise to mathematicians when it was discovered by Cantor in the 1870s.

Proof. The standard inclusions $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$ imply a chain of corresponding inequalities $\aleph_0 = |\mathbb{N}| \leq |\mathbb{Z}| \leq |\mathbb{Q}|$. Define a surjective mapping $\mathbb{N} \coprod \mathbb{N} \to \mathbb{Z}$ sending $(n, 1)$ to n and $(n, 2)$ to $-n$. By Theorem 8 it follows that

$$|\mathbb{Z}| \leq |\mathbb{N} \coprod \mathbb{N}| = \aleph_0 + \aleph_0 = \aleph_0,$$

so the result for $|\mathbb{Z}|$ follows from the Schröder – Bernstein Theorem.

Next define a surjective mapping $\mathbb{Z} \times (\mathbb{Z} - \{0\}) \to \mathbb{Q}$ sending (a, b) to a/b. We then have $|\mathbb{Q}| \leq |\mathbb{Z} \times (\mathbb{Z} - \{0\})| \leq \aleph_0 \cdot \aleph_0 = \aleph_0$. Once again the Schröder – Bernstein Theorem implies that $|\mathbb{Q}| = \aleph_0$.■

The next natural question concerns the cardinality of the set of the real numbers, and the result is again due to Cantor.

Theorem 12. *If* $\mathbb{R}$ *denotes the real numbers, then its cardinality satisfies* $|\mathbb{R}| = 2^{\aleph_0}$ *and therefore we have* $|\mathbb{R}| > \aleph_0$.

Proof. Usually this is derived using decimal expansions of real numbers, but we shall give a proof that does not involve decimals (although the idea is similar). The idea is to construct $1-1$ maps from $\mathbb{R}$ to $\mathbf{P}(\mathbb{N})$ and vice versa and then to apply the Schröder – Bernstein Theorem.

Let $\mathbf{D}: \mathbb{R} \to \mathbf{P}(\mathbb{Q})$ be the Dedekind cut map sending a real number **r** to the set of all rational numbers less than **r**. Since there is always a rational number between any two distinct real numbers, it follows that this map is $1-1$. Since $|\mathbb{Q}| = \aleph_0$, it follows that there is a $1-1$ correspondence from $\mathbf{P}(\mathbb{Q})$ to $\mathbf{P}(\mathbb{N})$, and the composite of **D** with this map gives the desired $1-1$ map from $\mathbb{R}$ to $\mathbf{P}(\mathbb{N})$.

Let $\mathbf{P}_\infty(\mathbb{N})$ denote the set of all ***infinite*** subsets of $\mathbb{N}$, and define a function from $\mathbf{P}_\infty(\mathbb{N})$ to $\mathbb{R}$ as follows: Given an infinite subset **B**, let $\mathbf{X}_\mathbf{B}$ be its characteristic function and consider the infinite series

$$\Sigma_B = \Sigma_k \, X_B(k) \cdot 2^{-k}.$$

This series always converges by the Comparison Test because its terms are nonnegative and less than or equal to those of the geometric series $\Sigma_k \, 2^{-k}$, which we know is convergent. Furthermore, different ***infinite*** subsets will yield different values (look at the first value of **k** that is in one subset but not in the other; if, say, **k** lies in **A** but not in **B**, then we have $\Sigma_A > \Sigma_B$. Note that all these sums lie in the interval $[0, 1]$ because $\Sigma_k \, 2^{-k} = 1$.

If **A** is a ***finite*** subset, consider the finite sum

$$\Sigma_B = 2 + \Sigma_k \, X_B(k) \cdot 2^{-k}.$$

Once again it follows that different finite subsets determine different real (in fact, rational) numbers. Furthermore, since the value associated to a finite set lies in the interval $[2, 3]$ it is clear that a finite set and an infinite set cannot go to the same real number. Therefore we have constructed a $1-1$ function from $\mathbf{P}(\mathbb{N})$ to $\mathbb{R}$.■

Since we have constructed $1-1$ mappings in both directions, we can apply the Schröder – Bernstein Theorem to complete the proof.

Finally, we prove another fundamental, well – known result about the cardinality of $\mathbb{R}^n$:

Theorem 13. *Given a set* **A**, *let* $\mathbf{A}^n$ *denote the* **n** *– fold product of* **A** *with itself. If* $\mathbb{R}$ *denotes the real numbers, then for all positive integers* **n** *we have* $|\mathbb{R}^n| = |\mathbb{R}|$.

One slightly nonintuitive consequence of this theorem is the existence of a $1-1$ correspondence between the points of the number line and the points on the coordinate plane. Of course, these objects with all their standard mathematical structures are quite different, but the theorem says that they cannot be shown to be distinct simply by means of transfinite cardinal numbers.

Using axiom(s) introduced in the next section, one can show that $n \cdot |A| = |A|$ and $|A^n| = |A|$ as above for every infinite set A and positive integer n, but here we shall outline a direct and relatively standard argument which does not depend upon the additional axiom(s).

Proof. There are two parts to the proof. The first is to verify the result when $n = 2$ and the second is to show that the case $n = 2$ implies the general case. The argument to prove the latter is essentially the same as in the Corollary to the Idempotent Laws for the cardinal number $\aleph_0$ (specifically, see Corollary 9).

We now concentrate on the case $n = 2$. The argument is based upon the existence of a $1-1$ correspondence

$$\{0,1\}^{\mathbb{N}} \to \{0,1\}^{N(0)} \times \{0,1\}^{N(1)}$$

sending a function $\mathbb{N} \to \{0,1\}$ to the ordered pair given by its restrictions to the even and odd natural numbers; clearly a function is completely determined by these restrictions, and conversely given functions on the even and odd natural numbers there is a unique way of assembling them into a function defined on all the natural numbers. This observation yields the cardinal number identity

$$2^{\aleph_0} = 2^{\aleph_0} \times 2^{\aleph_0}$$

and the validity of the theorem for $n = 2$ follows from this and the previously established identity $|\mathbb{R}| = 2^{\aleph_0}$.■

Corollary 14. *We also have* $2^{\aleph_0} = 2^{\aleph_0} + 2^{\aleph_0}$ *and* $2^{\aleph_0} = \aleph_0 \times 2^{\aleph_0}$.

Proof. These are consequences of the following chain of inequalities:

$$2^{\aleph_0} \leq 2^{\aleph_0} + 2^{\aleph_0} \leq \aleph_0 \times 2^{\aleph_0} \leq 2^{\aleph_0} \times 2^{\aleph_0} = 2^{\aleph_0}\blacksquare$$

Remark. The following generalizations of the usual laws of exponents also hold for cardinal numbers:

Theorem 15. (Transfinite Laws of Exponents). *If* α, β *and* γ *are (finite or transfinite) cardinal numbers, then we have* $\gamma^{\alpha+\beta} = \gamma^{\alpha} \cdot \gamma^{\beta}$, $(\gamma^{\alpha})^{\beta} = \gamma^{\alpha\beta}$, *and* $(\beta \cdot \gamma)^{\alpha} = \beta^{\alpha} \cdot \gamma^{\alpha}$.

The last two equations follow from the $1-1$ correspondences for function sets that were discussed in Section IV.5 (see Theorem IV.5.7), and the proof of the first follows from the analogous $1-1$ correspondence between $C^{A \sqcup B}$ and $C^A \times C^B$, a special case of which was discussed in the proof of Theorem 13 in this section.■

Applications to transcendental numbers

Cantor was led to develop set theory in his study of some basic questions about trigonometric series, and a few years after beginning this work he found a striking application to a longstanding problem of independent interest. We begin with the definitions needed to formulate the problem.

Definition. Let **x** be a real number. Then **x** is said to be ***algebraic*** if there is a nontrivial polynomial with rational coefficients (equivalently, integral coefficients; *cf.* the next paragraph) for which **x** is a root. A real number is said to be ***transcendental*** if it is not a root of any such polynomial.

Since every polynomial over the rational numbers can be written as an integral polynomial divided by a nonzero integer, it follows that a number is a root of a nontrivial polynomial over the rational numbers if and only if it is a root of a nontrivial polynomial over the integers.

Lemma 16. *If* **x** *and* **y** *are real numbers such that* **x** *is rational and* **y** *is transcendental, then their sum* **x** + **y** *is transcendental.*

Proof. Suppose that **x** + **y** is algebraic. Then there is a nontrivial polynomial **p** with rational coefficients which has **x** + **y** as a root. Dividing through by the (nonzero) coefficient of the highest degree term of **p** if necessary, we can assume that **p** is a monic polynomial. Express this monic polynomial as $t^n + q(t)$, where **q** has lower degree. Our hypotheses then imply that $(x + y)^n + q(x + y) = 0$. By the Binomial Theorem we may rewrite this as $y^n + r(y) = 0$, where **r(t)** is another polynomial of lower degree with rational coefficients. This implies that **y** is algebraic, contradicting our original assumption, and hence the only possibility is that **x** + **y** must be transcendental.■

Corollary 17. *If there is at least one transcendental real number, then the cardinality of the set* **T** *of transcendental real numbers satisfies* $\aleph_0 \leq |T|$.

Proof. Suppose that **y** is transcendental. Then one can define a mapping from the rational numbers $\mathbb{Q}$ to **T** sending $x \in \mathbb{Q}$ to $x + y \in T$. This mapping must be $1 - 1$ because $x + y = z + y$ implies $x = z$.■

In the next unit we shall prove a more general result about infinite cardinal numbers, but the preceding corollary gives us what we need for the time being.

In order to compare the algebraic and transcendental real numbers, we need to know the cardinality of the former, and it is given by the following result:

Theorem 18. *The set of all algebraic real numbers is countably infinite.*

Proof. **(*)** Since the set of algebraic real numbers contains the integers, it will suffice to show that the set of algebraic numbers is countable. For each positive integer **n** let A_n be the set of all real numbers **r** such that **r** is a root of a polynomial of degree **n** with rational coefficients. Since a countable union of countable sets is countable, it will suffice to show that each set A_n is countable.

Let P_n denote the set of all polynomials of degree **n**, and for each $p \in P_n$ let **W(p)** denote the set of real roots for **p**. Basic results on roots of polynomials show that each

set **W(p)** is finite. If we can show that $|W(p)| = \aleph_0$, it will follow that A_n is a countable union of the finite sets **W(p)**, where **p** runs through the elements of P_n, and hence A_n is countable.

Now a polynomial in P_n has the form

$$p(t) = a_n t^n + \ldots + a_1 t + a_0$$

where $a_n \neq 0$, and hence it is completely determined by the coefficients of the powers of the indeterminate, say **t**, ranging from **0** to the degree, which in this case is **n**. This means there is a canonical $1-1$ correspondence between P_n and $(\mathbb{Q} - \{0\}) \times \mathbb{Q}^n$ (where as usual $\mathbb{Q}$ denotes the rational numbers) which is given by taking the coefficients of t^k as **k** runs from **n** to **0**. Now we know that $|\mathbb{Q}| = \aleph_0$ by Proposition 11, and we also know that $|\mathbb{Q} - \{0\}| = |\mathbb{Q}|$ by Propositions 7 and 11, so that we have $|W(p)| = (\aleph_0)^{n+1}$. However, by Corollary 9 we also know that $(\aleph_0)^k = \aleph_0$ for all values of k, and this means that $|W(p)| = \aleph_0$ must be true. As noted before, this completes the proof of the theorem. ■

Historical remarks on transcendental numbers. It is not clear when mathematicians first considered the concept of a transcendental number, but various historical facts strongly suggest that this took place near the middle of the 17th century in connection with the results and viewpoints of R. Descartes (*cf.* page 343 of Burton). A few years later, J. Gregory (1638 – 1675) tried to show that both π and **e** were transcendental; however, his work had a small but irreparable error. Leibniz also concluded that π was transcendental but did not make a significant effort to prove this. Several 18th century mathematicians such as C. Goldbach (1690 – 1764), D. Bernoulli (1700 – 1782), J. H. Lambert (1728 – 1777), and A. – M. Legendre (1752 – 1833) had considered the possible existence of transcendental numbers, and there was a general agreement that numbers π and e should be transcendental although it was not clear how one might actually prove these statements. One important piece of evidence was the understanding at the time that some of the standard functions in calculus like $\sin x$ and e^x were not algebraic functions (*i.e.*, there is no nontrivial polynomial in two variables such that $P(x, f(x))$ is identically zero). We shall discuss this point in greater detail below. The existence transcendental numbers was first shown rigorously by J. Liouville (1809 – 1882) in the 1840s. Probably the best known example arising from his work is the so – called ***Liouville constant***:

$$c = \sum_{j=1}^{\infty} 10^{-j!} = 0.11000100000000000000001000\ldots.$$

The following online sites provide further information about Liouville's methods and results:

http://planetmath.org/encyclopedia/ExampleOfTranscendentalNumber.html

http://en.wikipedia.org/wiki/Liouville_number

During the next few decades, proofs that **e** and π were transcendental finally appeared; these results were due to C. Hermite (1822 – 1901) and F. Lindemann (1852 – 1939) respectively. Many other easily constructed numbers have been shown to be transcendental numbers since the original results of Liouville, but there are still many

open questions that are very easy to state but seem unlikely to be answered in the near future. The current state of affairs is summarized in the following online site:

http://mathworld.wolfram.com/TranscendentalNumber.html

The purpose of the preceding discussion is to put Cantor's result on transcendental numbers into perspective. At the time, the existence of such numbers had only recently been established, and the proofs required delicate manipulations of equations and inequalities. In contrast, Cantor's existence proof did not require any significant computations, but it also did not produce any explicit examples (although one can combine Cantor's diagonal process argument with Liouville's construction to describe an uncountable family of transcendental numbers). We should note that currently known results are still not adequate to answer many very easily stated questions; for example, whether πe or $\pi + e$ is transcendental (however, we do know that at least one of these numbers is transcendental).

Theorem 19. (Strong existence theorem for real transcendental numbers – Cantor). *The set of transcendental real numbers is nonempty, and its cardinality is equal to* $2^{\aleph_0}$.

Proof. As in the preceding discussion, the set of real numbers $\mathbb{R}$ splits into a union of the disjoint subsets **A** of algebraic real numbers and **T** of transcendental real numbers. Thus we have $|\mathbb{R}| = |A| + |T| = \aleph_0 + |T|$. If **T** were empty we would have $|\mathbb{R}| = \aleph_0$, and we know this is false by the results of Section 4. Therefore **T** must be nonempty, and by the lemma above it follows that there is a $1-1$ mapping from **A** into **T**; let T_0 denote the complement of its image, so that $|T| = |A| + |T_0| = \aleph_0 + |T_0|$. Therefore we have

$$|T| = \aleph_0 + |T_0| = \aleph_0 + \aleph_0 + |T_0| = \aleph_0 + |T| = |\mathbb{R}| = 2^{\aleph_0}.$$

We now indicate how one can use Cantor's result to answer one of the questions at the beginning of these notes in the very strong informal sense:

> *Almost every real number is transcendental. In particular, if one "chooses a real number at random," it will almost certainly be transcendental.*

Giving a mathematically precise definition of random choice is far beyond the scope of this course, but here is a discussion that can be made mathematically rigorous. Let us agree to restrict attention to real numbers in the closed unit interval $[0, 1]$. Given a reasonable subset **A** of the latter (these will include all countable subsets), one would like to estimate the probability that an element of the interval chosen at random will belong to **A**. If, say, we divide the interval into **n** nonoverlapping pieces of equal length, then the likelihood of choosing an element from one of the pieces should be just $1/n$. More generally, if we are given a subinterval of length **L** then the likelihood of choosing a point from the subinterval should be **L**.

How does this apply in our situation? Suppose that **B** denotes the algebraic numbers in the closed unit interval, so that **B** is countable by our previous results. Choose a $1-1$ correspondence with the natural numbers, and let $m > 0$ be an integer. For each **n**, let J_n be a subinterval of length $2^{-(m+n)}$ containing the n^{th} point in **B**. The likelihood that a chosen element will lie in **B** should be no greater than the likelihood that it will lie in the union of the intervals J_n and hence it should be no greater than the sums of the lengths of these intervals. We can use a geometric series argument to see that the latter sum is

equal to 2^{1-m}. Now **m** is arbitrary, so this means that the likelihood of randomly choosing an element from **B** is no greater than 2^{1-m} for every positive integer **m**, and hence (since it is nonnegative) this likelihood must be equal to zero. Informally, this means that if we pick a number from the unit interval at random, it is almost certain to be a transcendental number.■

Footnote on transcendental functions. In the discussion above we have asserted that certain basic functions such as trigonometric functions and exponential functions are transcendental. Since it is difficult to find statements or proofs of these facts written out explicitly, we shall explain how the proof for the usual exponential function follows from standard results on solutions to ordinary differential equations which are covered in lower division undergraduate courses and we shall give an online reference that considers the remaining elementary transcendental functions.

The first step is fairly simple.

Lemma 20. *Let* **f(x)** *be a continuous function on some interval. Then f is transcendental if and only if for every positive integer* **m** *the* $(m+1)^2$ *functions* $x^p \cdot f(x)^q$ *are linearly independent over the real numbers, where* $0 \le p, q \le m$.

Proof. The $(m+1)^2$ functions $x^p \cdot f(x)^q$ are linearly ***dependent*** over the reals if and only if there are coefficients $c_{p,q}$ which are not all zero such that $\sum c_{p,q}\, x^p \cdot f(x)^q = 0$. Thus if they are linearly dependent for some **m**, then there will be a nontrivial polynomial $G(x, y) = \sum c_{p,q}\, x^p y^q$ such that $G(x, f(x)) = 0$. Conversely, if we are given such a polynomial **G** and **m** is the highest power of **x** or **y** that appears, then it follows that the $(m+1)^2$ functions $x^p \cdot f(x)^q$ are linearly dependent over the real numbers. By the lemma, proving that the exponential function e^x is transcendental amounts to showing that the functions $x^p \cdot e^{qx}$ are linearly independent functions for $0 \le p, q \le m$, where **m** is an arbitrary positive integer. One relatively quick way to see this is to notice that the functions in question all satisfy an N^{th} order *homogeneous linear (ordinary) differential equation with constant coefficients*

$$D^N y + a_{N-1} D^{N-1} y + \ldots + a_1 D y + a_0 y = 0$$

where $N = (m+1)^{(m+1)}$ and $D^k y$ denotes the k^{th} derivative of **y**. Specifically, this is the equation for which the associated characteristic polynomial

$$p(t) = a_N t^N + a_{N-1} t^{N-1} + \ldots + a_1 t + a_0$$

is given by the following product:

$$p(t) = t^{m+1} (t-1)^{m+1} \ldots (t-m)^{m+1}$$

The linear independence of these solutions is a standard fact in the theory of ordinary differential equations, and in particular, the proof is described in Section 9.2 of the following representative textbook on the subject:

> W. F. Trench, ***Elementary Differential Equations***. Brooks/Cole (Thomson Learning), Pacific Grove CA, 2000. ISBN: 0–534–36841–7.

More specific references for the proof are essentially the entire content of pages 453 – 454 as well as Exercise 40 on page 457.

This linear independence result was essentially known in the 18th century to L. Euler (1707 – 1783), with some refinements of the concepts due to G. Monge (1746 – 1818) and A. – L. Cauchy (1789 – 1857).

The online document

http://math.ucr.edu/~res/math144/transcendentals.pdf

establishes similar results for the other so – called ***elementary transcendental functions*** that are studied in precalculus and calculus, and it provides some additional general perspective on determining when a function is algebraic or transcendental. Since the cited document uses material on extension fields from advanced undergraduate and beginning graduate courses, it is included mainly for reference purposes; although the main results are extremely well – known, it is extremely difficult to find a reference in which the various functions are actually proven to be transcendental.

Cardinal number problems for further consideration

Here are some natural questions that arise in connection with the results of this section. Some involve generalizations of these results, and others are simple questions about the arithmetic and ordering properties of cardinal numbers.

1. Is the partial ordering of cardinal numbers a linear ordering?
2. Is $\aleph_0$ the smallest transfinite cardinal number?
3. If **A** is an infinite set, does it follow that the idempotent identities $|\mathbf{A}| \cdot |\mathbf{A}| = |\mathbf{A}|$ and $|\mathbf{A}| + |\mathbf{A}| = |\mathbf{A}|$ always hold?
4. If there is a surjection from **A** to **B**, does it follow that $|\mathbf{B}| \leq |\mathbf{A}|$?
5. Given a cardinal number α, is there a unique minimal cardinal number β such that $\beta > \alpha$?

Most of these seem likely, and the final question is closely related to Cantor's terminology for transfinite cardinal numbers. For example, if the answers to this question and the first one are yes, then one can define $\aleph_1$ to be the unique minimal cardinal number strictly greater than $\aleph_0$, then take $\aleph_2$ to be the unique minimal cardinal number strictly greater than $\aleph_1$, and so on.

However, despite strong intuitive feelings that the preceding questions have affirmative answers, we are not yet equipped to answer such questions, and the material in the next two units is needed to provide answers. Before introducing this material, we shall devote the next section to a discussion of some ways in which Cantor's theory of sets was a radical departure from previous views of infinite objects in mathematics.

VI.5 : The impact of set theory on mathematics

Given the routine use of set theory throughout modern mathematics, it is easy to overlook the precedent – shattering nature of Cantor's legacy. The rest of this section provides some historical perspective.

It is not known exactly when questions about the concept of infinity first arose, but the well – known paradoxes due to Zeno of Elea (*c.* 490 – 430 B. C. E) indicate that ancient Greek philosophers and mathematicians recognized that difficulties arise when one attempts to discuss the infinite. The writings of Aristotle (384 – 322 B. C. E.) provided an effective way of confronting such questions by arguing that there were two kinds of infinity.

1. ***Actual infinity***, or ***completed infinity***, which Aristotle believed could not exist, is endlessness fully realized at some point in time.
2. ***Potential infinity***, which Aristotle maintained was manifest in nature — for example, in the unending cycle of the seasons or the indefinite divisibility of measurements — is infinitude spread over unlimited time and space.

This fundamental distinction between potential and actual infinity persisted in European mathematics for more than 2000 years.

However, the adoption of this distinction did not mean that speculation about infinity was absent from all of mathematics during that time. Speculations about infinity appeared in classical Indian mathematics, particularly in the writings of Bhaskara (also known as Bhaskara **II** or Bhaskaracharya, 1114 – 1185). By the end of the Middle Ages, various scientific, philosophical and theological questions about infinity received considerable attention in Europe as well as India and China. Many of the mathematical advances concerned summations of infinite series. With hindsight, it is apparent that the summation formulas for many series obtained during these centuries showed that the concept of completed infinity could be mathematically meaningful, at least in some contexts. Certain basic paradoxes and puzzles arose and provided further evidence that actual infinity was not an issue to be dismissed easily. Specific problems arise from many standard **1 – 1** correspondences between infinite sets and certain proper subsets; for example, between the nonnegative integers and the even nonnegative integers. These constructions seemed to contradict a commonsense idea that appears in Euclid: ***The whole is always greater than any of its (proper) parts.*** The writings of Galileo (G. Galilei, 1564 – 1642) on such problems were the first to suggest a more enlightened attitude toward the infinite; in particular, he proposed that *"infinity should obey a different arithmetic than finite numbers."* We have seen that one version of Galileo's idea plays an important role in Cantor's work. However, during the nearly three centuries between Galileo and Cantor, mathematicians managed to avoid confronting questions about infinity for the most part. By confining their attention to Aristotle's potential infinity, mathematicians were able to address problems and develop crucial concepts including infinite series, limit, and infinitesimals [*sic*], and thus to develop calculus without having to grant that infinity itself was a mathematical object. In fact, early in the 19th century the highly eminent mathematician C. F. Gauss (1777 – 1855) expressed his "horror of the actual infinite" in the following terms:

> I protest most vehemently against the use of infinite magnitude as something completed, which is never permissible in mathematics. The infinite is merely a figure of speech, the true meaning being a limit which certain ratios approach as closely as we wish, while others may be permitted to increase beyond all bounds.

Even Cantor admitted that considering infinite sets as single entities — not as merely going on forever but as completed objects — was a concept to which he had been "logically forced, almost against my will." This erasing of the distinction between potential and actual infinities was "in opposition to traditions that had become valued."

Cantor's ideas generated considerable opposition and controversy for several reasons. For many mathematicians, the sets themselves were less disturbing than the uses to which Cantor put them; some mathematicians were particularly uneasy with Cantor's proof showing that "almost every" real number is transcendental; ***i.e.***, they are not roots of polynomial equations with rational coefficients. As noted in the discussion of Cantor's result, a considerable amount of intricate calculation is needed to prove that there are transcendental numbers and to verify the "obvious facts" that familiar numbers like e and π are transcendental. Cantor's existence proof required no significant computations at all, and in some respects it looks as if one is getting something for nothing. Of course, one reason the argument is so simple is that it does not provide any way of deciding whether a given number is algebraic or transcendental.

Cantor's result on transcendental numbers was the first important example of what has come to be called a ***pure – existence proof***. Giving not the slightest hint of how to construct even a single transcendental number, it established the existence of a host of such numbers by proving that it would be contradictory for them not to exist. Once again the basic issue is infinity. A proof by *reductio ad absurdum* that establishes the existence of an object in a finite set is perfectly acceptable to any mathematician; in principle, one can always produce the object by checking all the members of the set.

But the same is not true for, say, the transcendental numbers, which belong to the infinite set of real numbers. For this reason many mathematicians rejected Cantor's proof completely, objecting that a contradiction was no substitute for a tangible example.

In fact, some mathematicians were unwilling to accept Cantor's entire approach, which challenged established mathematical principles like the previously mentioned avoidance of actual or completed infinity. For example, H. Poincaré (1854 – 1912) expressed his disapproval in a statement that Cantor's set theory would be considered by future generations as "a disease from which one has recovered." Much stronger criticism was voiced by L. Kronecker (1823 – 1891), who strongly maintained that the appropriate objects for mathematical study were those that could be realized in a fairly concrete fashion (for example, his views excluded transcendental numbers entirely). Such a perspective leaves little place for the explicit treatment of "actual infinity" that permeates Cantor's work.

On the other hand, not all leading mathematicians were opposed to Cantor's ideas. Some highly eminent mathematicians such as G. Mittag – Leffler (1846 – 1927), K. Weierstrass (1815 – 1897), and long – time friend R. Dedekind supported Cantor's ideas and defended them against his critics. Aside from the revolutionary nature of Cantor's ideas, another reason for reservations about them was that some key concepts were initially expressed in a somewhat imprecise fashion, and yet another was that some basic questions about manipulating infinite sets turned out to be far more challenging

than they seemed at first; some issues are discussed in the fourth paragraph of Section 3. Unfortunately, the strain of the controversy over Cantor's work ultimately inflicted an extremely heavy toll on him, both personally and professionally.

Of course, our use of Cantor's ideas today and our presentation of his existence proof for transcendental numbers both indicate that his methods and results were increasingly accepted as mathematically valid (but in many cases this acceptance was reluctant). In particular, during the years immediately following Cantor's work, some mathematicians solved some other fundamental problems using pure, nonconstructive existence proofs; the most striking result of this sort called the ***Hilbert Basis Theorem*** was obtained by D. Hilbert (1862 – 1943) in 1889. A statement of this result requires concepts well beyond the scope of this course, but for the sake of completeness here is an online reference to one fundamental but (relatively) elementary class of special cases:

http://en.wikipedia.org/wiki/Hilbert's_basis_theorem

Hilbert was one of the most influential mathematicians of his time, and his acceptance of Cantor's work reflected the incorporation of set theory into the mainstream of mathematics. The following frequently quoted statement states his position strongly but concisely: ***No one shall expel us from the paradise that Cantor has created.***

Hilbert addressed concerns about increasing abstraction by stressing the vast amount that could be done if one adopts such an approach in contrast to the relatively limited amount that could be done if one does not. To most mathematicians in the early 20th century, Hilbert's formalist viewpoint offered an attractive viewpoint, and a largely dominant majority of present day mathematicians also take a modified formalist view towards the subject. These modifications are necessary because of the fundamental incompleteness results due to K. Gödel that will be discussed in the next unit.

VI. 6 : Transfinite induction and recursion

(Halmos, §§ 12 – 13, 17 – 20; Lipschutz, §§ 8.1 – 8.9, 8.12 – 8.13)

This section has two objectives. The first is to formulate concepts of

(1) proof by transfinite induction,

(2) definition by transfinite recursion,

which apply to well – ordered sets that are larger than the nonnegative integers. The second aim is to summarize the basic properties of ordinal numbers that are used most often in mathematics.

The proofs of many crucial results on well – ordered sets are considerably less elementary than most of the material in these notes. In particular, at several steps one needs slightly stronger versions of some axioms and definitions than we have stated in these notes. Precise statements appear in the book by Goldrei cited at the beginning of the first unit of these notes; in cases where we have stated simplified versions of axioms, we have done so for the sake of clarity and because the simpler versions are

adequate for nearly everything one wishes to do in other branches of mathematics. Finally, for most mathematical purposes the theory of well – ordered sets are mainly significant as means to some other end, and such objects play less of direct role in other branches of mathematics than the other material discussed in these notes. For these reasons, **we shall not attempt to give all the details of the more complicated proofs here, but instead we shall describe some of the arguments and give references to the book by Goldrei. None of the subsequent material in these notes will depend upon the results that are stated without complete proofs.**

Given the relative difficulty of some material in this section, the following suggestions might be helpful. The most important thing to do is to concentrate on understanding the definitions and statements of the main results. This should provide enough information to read the remaining sections in these notes. When these points are understood, a natural second step is to understand the outlines and main ideas of the proofs well enough to be able to summarize or explain them. For the purposes of this course, the final level of mastery is to have a full understanding of all the steps in the proofs.

Traditionally the elements of a well – ordered set are denoted by expressions involving nonnegative integers and Greek letters, and we shall follow this convention here.

Notational conventions. Suppose that X is a well – ordered set. The least element of X will be denoted by 0 or by 0_X when it is necessary to stress the dependence upon X. If $\alpha \in X$, the ***initial segment*** associated to α is the set of all β such that $\beta < \alpha$, and it is denoted by $[0, \alpha)$ or less ambiguously by $[0, \alpha)_X$. Likewise, we define the ***closed interval*** $[0, \alpha]$ to be the set of all β such that $\beta \leq \alpha$. Given a well – ordered set X, its ***immediate successor*** $X + 1$ is the set $X \cup \{X\}$ with the original well – ordering on X and the added element X strictly greater than every $\alpha \in X$. Recall that we have constructed set theory so that no set will be a member of itself, and thus it follows that X is distinct from each $\alpha \in X$.

Transfinite induction and recursion

Transfinite induction is an adaptation of proof by mathematical induction to include (large) well-ordered sets. Before describing this principle it will be useful to make the following elementary observation.

Proposition 1. *Let X be a well – ordered set, and let $\alpha \in X$. Then exactly one of the following is true*:

(1) *There is a $\beta \in X$ such that α is the first element in X that is strictly larger than β, and α is not the least upper bound of all elements of X that are strictly less than α.*

(2) *For each β such that $\beta < \alpha$ there is some $\gamma \in X$ such that $\beta < \gamma < \alpha$, and α is the least upper bound of all elements of X that are strictly less than α.*

Proof. If the first holds, then β is the least upper bound of all elements of X that are strictly larger than α. Suppose now that the second holds. Clearly α is an upper bound for the set in question. To see that it is the least upper bound, note that if $\beta < \alpha$ then β cannot be an upper bound because there is always some γ such that $\beta < \gamma < \alpha$. ■

Notation. Elements of the first type are called ***(immediate) successor elements*** (and one often writes $\alpha = \beta + 1$ or $\alpha = \beta^+$ in this case), and elements of the second type are called ***limit elements.***

We now proceed to the main results.

Theorem 2 (Principle of transfinite induction**).** *Let* $\mathbf{X}$ *be a well – ordered set, and suppose that for each* $\alpha \in \mathbf{X}$ *we are given a statement* $\mathbf{S}(\alpha)$ *such that the following conditions hold*:

(1) *If* $\mathbf{0_X}$ *denotes the unique minimum element of* $\mathbf{X}$, *then* $\mathbf{S}(\mathbf{0_X})$ *is true.*

(2) *For each* β *in* $\mathbf{X}$, *if* $\mathbf{S}(\gamma)$ *is true for all* $\gamma < \beta$, *then* $\mathbf{S}(\beta)$ *is also true.*

Then $\mathbf{S}(\alpha)$ *is true for every* $\alpha \in \mathbf{X}$.

Proof. The argument is similar to the one for finite induction. Suppose that at least one of the statements is false. Then there is a unique minimum α_0 such that $\mathbf{S}(\alpha_0)$ is false. Since $\mathbf{S}(\mathbf{0_X})$ is true we know that $\alpha_0 \neq \mathbf{0_X}$ and thus the set of all β such that $\beta < \alpha$ must be nonempty. For each such β the statement $\mathbf{S}(\beta)$ is true, and therefore by the second condition we know that $\mathbf{S}(\alpha_0)$ is also true. Now this contradicts our choice of α_0, and the problem arises from our assumption that at least one of the statements $\mathbf{S}(\alpha)$ is false. Thus all of the statements must be true.■

In practice, the verification of the second condition often splits into two cases: One for successor elements (those which have an immediate predecessor), where the usual inductive approach can be applied to show that $\mathbf{P}(\gamma)$ implies $\mathbf{P}(\gamma + 1)$, and the case for limit elements, which have no predecessor, and thus cannot be handled by such an argument.

Typically, the case for limit ordinals is handled by noting that a limit element β is the least upper bound of all elements $\gamma < \beta$ and using this fact to prove $\mathbf{P}(\beta)$ assuming that $\mathbf{P}(\gamma)$ holds true for all $\gamma < \beta$.

Transfinite recursion is closely related to transfinite induction, but the latter is a method of ***proof*** and the former is a method of ***definition*** or of ***construction***. The basic idea is fairly simple. We start with a well – ordered set Λ and specify the object for the zero (least element), then assuming we know how to define the object indexed by γ for every $\gamma < \alpha$, we use this partial function to find $\mathbf{f}(\alpha)$. In a little more detail, one defines a family of objects indexed by the well – ordered set $\mathbf{X}$ — say $\mathbf{B}_\alpha$, for every $\alpha \in \mathbf{X}$, or perhaps every α less than some bound ξ — by specifying three things:

(1) What $\mathbf{B_0}$ is.

(2) How to determine $\mathbf{B}_{\alpha+1}$ from $\mathbf{B}_\alpha$ (or possibly from the entire sequence up to $\mathbf{B}_\alpha$).

(3) For a limit element α, how to determine $\mathbf{B}_\alpha$ from the sequence of previously determined $\mathbf{B}_\gamma$ for $\gamma < \alpha$.

Formally there is not much formal difference between the second and third items, but in practice they are so often distinct that it is useful to present them separately.

Here is the formal statement.

Theorem 3. (Transfinite Recursive Definition Theorem.) *Suppose that* X *is a well – ordered set and* B *is a set which does not necessarily have any additional structure. Assume also that for* $\alpha \in X$ *we have a function* $H : B^{[0,\alpha)} \to B$, *and let* $z_0 \in B$. *Then there is a unique function* $f : X \to B$ *such that* $f(0) = z_0$ *and for all positive* n *we have*

$$f(\alpha) = H\big(f \,|\, [0, \alpha)\big).$$

Proof. The approach is parallel to the proof of the (Finite) Recursive Definition Theorem in Section V.2. We first prove existence by defining a sequence of functions $g_\alpha : [0, \alpha] \to B$ which agree on the overlapping subsets, and then we construct a function g whose graph is the union of the graphs of the partial functions. The uniqueness proof will then reduce to proving uniqueness for the restrictions to each subset $[0, \alpha]$.

The function $g_0 : \{0\} \to B$ is defined by $g_0(0) = z_0$. Suppose we are given the functions $g_\beta : [0, \beta] \to B$ for $\beta < \alpha$, where one has the compatibility $g_\beta = g_\beta \,|\, [0, \gamma]$ for $\gamma < \beta$. Since $[0, \alpha) = \cup_{\beta < \alpha} [0, \beta]$ it follows that we can define a function k_α on the left hand side whose restriction to each subset $[0, \beta]$ is g_β. We can extend this to a function g_α the closed interval $[0, \alpha]$ by setting $g_\alpha(\delta)$ equal to $H(k_\alpha)$. Let f be the function whose union is the graphs of the functions g_α for all $\alpha \in X$. By construction this function has the properties specified in the theorem.

To conclude the proof, we need to show uniqueness. Suppose that f' is an arbitrary function satisfying the given properties, and let f be constructed as in the previous paragraphs. Suppose that $f \neq f'$. By hypothesis both agree at zero, so there exists a unique minimal element $\alpha > 0$ at which their values disagree. In particular, the functions agree on the initial segment $[0, \alpha)$, and thus by the displayed condition we have

$$f(\alpha) = H\big(f \,|\, [0, \alpha)\big) = H\big(f' \,|\, [0, \alpha)\big) = f'(\alpha),$$

where the first equation is true by construction, the second is true by the minimality hypothesis on α, and the third is true by the assumption on f'. This contradicts our assumption that the two functions had different values at α, and it follows that there cannot be a point where the values of the two functions are unequal. ■

Comparison of well – ordered sets

The following basic fact about well – ordered sets is extremely important for many purposes, and it illustrates the concept of definition by transfinite recursion.

Theorem 4. *Let* X *and* Y *be well – ordered sets. Then there exists a nondecreasing map* $f : X \to Y + 1 = Y \cup \{Y\}$ *such that the following hold*:

(1) *If* $X_0 = f^{-1}[Y]$, *then* $f \,|\, X_0$ *is strictly increasing.*

(2) *If* $\alpha \in X_0$, *then* f *defines a* $1 - 1$ *order – preserving correspondence between the initial segments* $[0_X, \alpha)$ *and* $[0_X, f(\alpha))$.

(3) *If* $f(\alpha) = Y \in Y + 1 = Y \cup \{Y\}$ *then* $f(\beta) = Y$ *and* $f\big[[0_X, \alpha)\big] \supset Y$.

Proof. We construct the map **f** by transfinite recursion, beginning with $f(0_X) = 0_Y$. Suppose that $\alpha > 0_X$ and one has $g_\alpha = f|[0, \alpha)$ is defined with the given properties on $[0, \alpha)$. By construction, if $g_\alpha(\beta) \in Y$ then $g_\alpha[[0, \beta)] \subset Y$. There are now two cases.

Case A. $g_\alpha(\beta) \neq Y$ for all $\beta \in [0, \alpha)$. **CLAIM:** Either there is an upper bound for the image of g_α or else $g_\alpha([0, \alpha)) = Y$ for some $\beta < \alpha$. If the second alternative is false, then g_α is not onto, so let γ be an element not in the image. Furthermore, we claim that no δ satisfying $\delta > \gamma$ can be in the image. If it were, then the second property would imply that γ would also be in the image. Therefore γ must be an upper bound for the image of g_α. Extend the definition of g_α to include α by taking $g_\alpha(\alpha)$ to be the least element of **X** that is not in the set $g_\alpha([0, \alpha))$.

Case B. $g_\alpha(\beta) = Y$ for some $\beta < \alpha$. In this case we extend the definition of g_α to include α by setting $g_\alpha(\alpha) = Y$.

Thus we have constructed a map g_α on $[0, \alpha]$ and it is an elementary exercise to show it has the desired properties.■

The preceding result has the following important consequence; text references are page 73 of Halmos and Theorem 8.10 on page 207 of Lipschutz.

Theorem 5. *Let* **X** *and* **Y** *be well – ordered sets. Then either there is a* $1 - 1$ *order – preserving map from* **X** *to* **Y** *or else there is a* $1 - 1$ *order – preserving map from* **Y** *to* **X**. *In each case one can choose the mapping so that its image is an initial segment or the whole set.*

Proof. Let **f** be as in the previous result. There are two possibilities.

Case A. Suppose that $f[X] \subset Y$. — In this situation there are two subcases. If the image is equal to **Y**, then f is a $1 - 1$ order – preserving correspondence between **X** and **Y**, so both options are realized in this case. Suppose now that the image is a proper subset. Then **f** defines a $1 - 1$ order – preserving map from **X** to **Y**. We claim that the image is in fact an initial segment. Let γ be the least element of **Y** not in the image, and suppose that $f(\beta) < \gamma$. By the previous result, we know that $f[[0, \beta)] \subset Y$, and therefore it follows that the image of **f** is equal to $[0, \gamma)$.

Case B. Suppose that $Y \in f[X]$. — Let γ be the least element in $f^{-1}[Y]$. Then **f** defines a $1 - 1$ order – preserving correspondence from $[0, \alpha)$ to **Y**, and the inverse defines a similar map from **Y** to the initial segment $[0, \alpha)$ of **X**.■

Types of well – ordered sets

Definition. If $(X, \leq_X)$ and $(Y, \leq_Y)$ are well – ordered sets, then we shall say that they have the *same well – order type* if there is an order – preserving $1 - 1$ correspondence from **X** to **Y**. We frequently denote this relationship by $|X, \leq_X| = |Y, \leq_Y|$.

It is probably not surprising that this relation is reflexive, symmetric and transitive, so we shall do so right away.

Proposition 6. *For every well – ordered set* $(X, \leq_X)$ *we have* $|X, \leq_X| = |X, \leq_X|$. *Furthermore, if* $(X, \leq_X)$ *and* $(Y, \leq_Y)$ *are such that* $|X, \leq_X| = |Y, \leq_Y|$, *then* $|Y, \leq_Y| = |X, \leq_X|$. *Finally, if* $(X, \leq_X)$, $(Y, \leq_Y)$ *and* $(Z, \leq_Z)$ *satisfy* $|X, \leq_X| = |Y, \leq_Y|$ *and* $|Y, \leq_Y| = |Z, \leq_Z|$, *then* $|X, \leq_X| = |Z, \leq_Z|$.

Proof. For every partially ordered set $(X, \leq_X)$, the identity map $\mathbf{id}_X$ is an order – preserving $1 - 1$ correspondence from X to itself, so the relationship is reflexive. Similarly, if we have $|X, \leq_X| = |Y, \leq_Y|$ and f is the associated $1 - 1$ correspondence from X to Y, then its inverse is an order – preserving $1 - 1$ correspondence from Y to X. If in addition we have $|Y, \leq_Y| = |Z, \leq_Z|$ with an associated $1 - 1$ correspondence g from X to Y, then the composite $g \circ f$ is an order – preserving $1 - 1$ correspondence from X to Z.■

Definition. If $(X, \leq_X)$ and $(Y, \leq_Y)$ are well – ordered sets, then we shall say that the *well – order type of* $(X, \leq_X)$ *is smaller than or equal to the order type of* $(Y, \leq_Y)$ if there is an order – preserving $1 - 1$ map from X to Y whose image is an initial segment of Y. We frequently denote this relationship by $|X, \leq_X| \leq |Y, \leq_Y|$.

We shall show that the relationship in the preceding paragraph behaves like a linear ordering. Most of the properties are easy to check, but proving the relationship is antisymmetric requires the following input (*cf.* Lipschutz, Theorem 8.9, page 207):

Proposition 7. *Let* X *be a well – ordered set. Then there is no* $1 - 1$ *strictly increasing mapping from* X *to itself whose image is an initial segment* $[0, \alpha)$ *for some* $\alpha \in X$.

Proof. Suppose that there is such a map, and denote it by f. Since f is not onto, it cannot be the identity. On the other hand, by hypothesis we also have $f(0_X) = 0_X$. Therefore there must be a first β such that $f(\beta) \neq \beta$. Since $f(\gamma) = \gamma$ for $\gamma < \beta$ and β is the first element which is not in $[0, \beta)$, it follows that $f(\beta) \geq \beta$. In fact, strict inequality hold because $f(\beta) \neq \beta$. Since $f(\beta)$ lies in the image of f, which is equal to $[0, \alpha)$, it follows that $f(\beta) < \alpha$, and thus also that $\beta \in [0, \alpha)$ so that β lies in the image of f. Suppose that $f(\gamma) = \beta$. What can we say about γ? First of all, it cannot be less than β, for $\gamma < \beta$ implies $f(\gamma) = \gamma < \beta$. However, it also cannot be greater than or equal to β, for then we must have $\beta < f(\beta) \leq f(\gamma)$. This is a contradiction, which we can trace back to our assumption about the image of f. It follows that every strictly increasing mapping from the well – ordered set X to itself must be onto.■

Theorem 8. *The relationship* $\leq$ *on well – ordering types has the following properties*:

> **(1)** *For every well – ordered set* $(X, \leq_X)$ *we have* $|X, \leq_X| \leq |X, \leq_X|$. *Furthermore, if the well – ordered sets* $(X, \leq_X)$, $(Y, \leq_Y)$ *and* $(Z, \leq_Z)$ *satisfy* $|X, \leq_X| \leq |Y, \leq_Y|$ *and* $|Y, \leq_Y| \leq |Z, \leq_Z|$, *then* $|X, \leq_X| \leq |Z, \leq_Z|$.
>
> **(2)** *If* $(X, \leq_X)$ *and* $(Y, \leq_Y)$ *are well – ordered sets such that* $|X, \leq_X| \leq |Y, \leq_Y|$ *and* $|Y, \leq_Y| \leq |X, \leq_X|$, *then* $|Y, \leq_Y| = |X, \leq_X|$.
>
> **(3)** *If* $(X, \leq_X)$ *and* $(Y, \leq_Y)$ *are well – ordered sets, then we have either* $|X, \leq_X| \leq |Y, \leq_Y|$ *or* $|Y, \leq_Y| \leq |X, \leq_X|$.

Proof. The proofs of the first assertions are similar to the corresponding arguments for order types. For the reflexive property we can use the identity mapping on **X**, and for the transitivity property, we are given strictly increasing mappings **f** and **g**, and the required map from **X** to **Z** is the composite $g \circ f$. The dichotomy property in the third assertion is an immediate consequence of Theorem 5 from the previous subsection. Thus it only remains to prove the antisymmetric property which is stated in the second assertion.

Suppose that $|X, \leq_X| \leq |Y, \leq_Y|$ and $|Y, \leq_Y| \leq |X, \leq_X|$, and suppose that $f : X \to Y$ and $g : Y \to X$ are the strictly increasing mappings onto the whole set or an initial segment. By the preceding result, the composite $g \circ f$ is the identity mapping. If we can prove that **g** is onto, then the conclusion will follow because then **g** will be a $1 - 1$ onto order – preserving map, and hence we have $|Y, \leq_Y| = |X, \leq_X|$. To verify that the mapping **g** is onto, let $x \in X$ be arbitrary and note that $g \circ f = \mathrm{id}_X$ yields $x = g(f(x))$. ■

Ordinal numbers

Grammarians distinguish between two types of numbers in a language; namely, the ***cardinal numbers*** like *one, two, three, …* which we use to count objects, and the ***ordinal numbers*** like *first, second, third, …* which we use to order objects or concepts. Both notions of numbers are also present in set theory, and in fact Cantor introduced transfinite ordinal numbers before he introduced transfinite cardinal numbers.

In set theory, the relationship between ordinal and cardinal numbers is not quite the same as it is in ordinary language, but the fundamental pairing of cardinals with counting and ordinals with ordering carries over. We have seen that a cardinal number in mathematics in some sense corresponds to an equivalence class of sets in $1 - 1$ correspondence with each other. One way of describing an ordinal number in mathematics is that in some sense it corresponds to an equivalence class of well – ordered sets. More precisely, given two well – ordered sets $(A, <_A)$ and $(B, <_B)$, then we shall say that they have the same ***ordinal type*** (or represent the same ***ordinal number***) if there is a $1 - 1$ order preserving correspondence between them; ***i.e.***, there is a $1 - 1$ correspondence $f : A \to B$ that is *strictly increasing*: For all **x** and **y**, $x <_A y$ implies $f(x) <_B f(y)$ for all **x** and **y** in **A**. It follows that the inverse map $f^{-1} : B \to A$ will also be strictly increasing in this case.

The simplest examples of well – ordered sets are given by subsets of the natural numbers; specifically, for each nonnegative integer **n** we can take the well – ordered set with **n** elements given by $\{0, \ldots, n - 1\}$ or we can take the entire set of natural numbers. Not surprisingly, the example with **n** elements is denoted by **n**, and following Cantor the well – ordered set given by the natural numbers is generally denoted by ω. However, there are also many other examples that one can construct from these. Perhaps the simplest one is the successor $\omega + 1$, which as before is given by the union

$$\omega \cup \{\omega\}$$

with the original ordering on the elements of ω and the extra element ω as a unique maximal element. Of course, one can repeat this process and obtain a new successor set $\omega + 2 = (\omega + 1) + 1$, and this can be taken further to define a sequence of well – ordered sets $\omega + n$ for every positive integer **n**. In fact, there are standard, general

arithmetic operations for constructing new well – ordered sets out of old ones. The discussions on pages 75 – 77 and 81 – 85 of Halmos and Sections 8.10 – 8.12 on pages 209 – 213 of Lipschutz provide both simple and complicated examples of how these constructions can be combined.

Aside from the successor construction taking a well – ordered set **X** to its successor set **X + 1,** we shall not need the arithmetic operations on well – ordered sets in these notes. However, the previously cited discussions in Halmos and Lipschutz imply the existence of many inequivalent well – ordered sets that are countably infinite, and of course it would be helpful to have some comprehensive means for keeping track of such objects.

The ordinal numbers will be a special class of well – ordered sets with the following crucial property: ***Every well – ordered set has the well – ordering type of a unique ordinal number.***

Originally Cantor attempted to define ordinal numbers using the previously mentioned approach with well – ordering types of well – ordered sets. However, the following definition due to J. von Neumann improves on Cantor's approach in several respects and has become the standard mathematical description for ordinal numbers (***e.g.***, it is the formulation appearing page 75 of Halmos; in contrast, the formulation on page 208 of Lipschutz is essentially Cantor's definition):

Definition. A set **S** is an ***ordinal*** if and only if **S** is well – ordered with respect to set membership and every element of **S** is also a subset of **S;** in other words, $x \in S$ implies $x \subset S$. The class of all ordinals (the ***ordinal numbers***) will often be denoted by Ω; the standard form of the Axiom of Specification (which is slightly different from the one in these notes) implies that Ω is a class. In Proposition 11 below shall prove that Ω cannot be a set (this is the *Burali – Forti Paradox* that we have previously mentioned).

The motivation for this definition arises from a ***standard model for the Peano axioms*** in which each nonnegative integer **n** corresponds to an explicit set with exactly **n** elements:

0 is represented by the empty set $S_0 = \varnothing$.
1 is represented by the one element set $S_1 = \{\varnothing\}$.
2 is represented by the two element set $S_2 = \{\varnothing, \{\varnothing\}\} = S_1 \cup \{S_1\}$
3 is represented by the set $S_3 = \{\varnothing, \{\varnothing\}, \{\varnothing,\{\varnothing\}\}\} = S_2 \cup \{S_2\}$

$\ldots$

n is represented by the **n** element set $S_n = S_{n-1} \cup \{S_{n-1}\}$

Each of the sets S_n satisfies the definition of an ordinal, and the same is true of the union $S_\omega = \cup_n S_n$. Additional motivation for the definition is that if **S** is an ordinal, then the successor set $S + 1 = S \cup \{S\}$ is also an ordinal.

Proposition 9. *If* **S** *is an ordinal and* $x \in S$, *then* **x** *is also an ordinal.*

Proof. By the basic condition on ordinals, **x** is a subset of **S,** and therefore $y \in x$ implies $y \in S$. We need to show that **x** is well – ordered with respect to set membership and every element of **x** is also a subset of **x.** If **A** is a nonempty subset of **x,** then the definition of ordinal number implies that $A \subset x \subset S$, and therefore the set **A** has a least element with respect to set membership because **S** is well – ordered. Now

suppose that $y \in x$; to show that $y \subset x$ we need to show that if $z \in y$ then $z \in x$. We claim that $z \in S$; if so, then all three of **x, y** and **z** lie in **S,** and since the ordinal **S** is linearly ordered by set membership we must have $z \in x$.

To prove that $z \in S$, note that $y \in S$ by the preceding paragraph, and since **S** is an ordinal it follows that **y** is a subset of **S,** so that $z \in S$ as required.■

Fundamental properties of ordinal numbers

The first result in this subsection might look as if it should be trivial, and it would be if we knew that the class of ordinals Ω was a set. However, at this point we do not know whether this is true (and in fact Proposition 11 below will show that Ω is **not** a set).

Theorem 10. *If Ω denotes the ordinal numbers with the relation given by set membership, then every nonempty subset in Ω has a least element.*

Proof. Let **X** be a nonempty set of ordinals, and let $\alpha \in X$. Take **Y** to be the set of all $\beta \in Y$ such that $\beta \in \alpha$. If **Y** is empty, then α is the least element of **X** because **X** is linearly ordered by set membership. If **Y** is nonempty, then **Y** is contained in α (using linear ordering again) and as such it has a least element. Thus we have found a least element in both cases.■

We have already noted that there is no "set of all ordinal numbers" just as there is no "set of all cardinal numbers." In fact, the paradox about ordinals was noticed by C. Burali – Forti (1861 – 1931) a few years before Cantor discovered the analogous paradox about cardinal numbers.

Proposition 11 (Burali – Forti Paradox**).** *The class Ω of ordinal numbers is not a set.*

Proof. Suppose that Ω is a set. We claim that it is an ordinal; since we have shown that it is well – ordered with respect to set – theoretic membership, it follows that the latter describes a well – ordering on Ω. To prove the second condition for an ordinal, let $S \in \Omega$; we need to show that $S \subset \Omega$, or equivalently that $x \in S$ implies $x \in \Omega$. But this follows because every element of an ordinal is an ordinal.

Since Ω is an ordinal, it follows that $\Omega + 1$ is also an ordinal, and hence $\Omega + 1$ is an element of Ω. By construction we have $\Omega \in \Omega + 1$, and since Ω is an ordinal it follows that $\Omega \in \Omega$, which contradicts the Axiom of Foundation. The contradiction arises from our assumption that Ω is a set, and therefore the latter must be false.■

The following basic fact has already been mentioned.

Theorem 12 (Classification of Well – Ordered sets**).** *Let **X** be a well ordered set. Then there is a unique $\alpha \in \Omega$ for which there is a $1 - 1$ order – preserving correspondence from **X** to α.*

Sketch of Proof. (See Goldrei, Theorem 8.2, pages 206 – 207, and Theorem 8.5, pages 212 – 213, for further details.) We start with existence. The idea is to construct a mapping from **X** to the ordinals by transfinite recursion such that for all $\beta \in X$, the

function **f** maps **[0, β)** in **X** to **[0, f(β))** in **Ω.** Eventually this process terminates when one runs out of elements in **X.** Since **Ω** is not a set, there are elements of it that do not lie in the image of **f,** and if **α** is the first element not in the image of **f,** then the latter defines a **1 – 1** order – preserving correspondence from **X** to **α.**

Uniqueness follows from our previous result that a well – ordered set cannot be in **1 – 1** order – preserving correspondence with a proper subset of itself.■

The following existence result for least upper bounds is important for many purposes.

Theorem 13. *Let* **X** *be a nonempty set of ordinals. Then* **X** *has an upper bound (in the class of ordinals).*

Corollary 14. *In the above situation, the set* **X** *has a least upper bound.*

The corollary follows because the ordinals are well – ordered.■

Sketch of proof of upper bound theorem. (See Goldrei, Theorem 9.4, page 209, or Halmos, the first four lines of page 80, for further details.) Let **$(X)** be the union of all ordinals in **X.** To complete the proof, it is necessary to show that **$(X)** is an ordinal and that it is an upper bound for all the ordinals in **X.** The second part uses the fact that two ordinals **α** and **β** satisfy the condition **α ∈ β** if and only if **α** is a proper subset of **β.** This fact is established in (solved) Exercise 8.6 on page 208 of Goldrei.■

Theorem 15. (Hartogs' Theorem.) *Given a set* **A,** *there is an ordinal* **β** *such that there is no* **1 – 1** *mapping from* **β** *into* **A.**

This result strongly suggests that for every set **A** there is an ordinal **λ** for which we have the cardinal number inequality **|A| ≤ λ.** This will follow from the results of the next section, but the proof is considerably less trivial than it might seem at first; the problem involves proving the existence the **1 – 1** function from **A** to **β** whose existence may seem intuitively clear.

Notes. We have followed Goldrei in calling this result Hartogs' Theorem, but we must add a **STRONG WARNING** that **usually "Hartogs' Theorem" refers to a major result in the theory of functions of several complex variables** due to F. Hartogs (1874 – 1943).

Proof of Hartogs' Theorem on Ordinals. We shall only sketch the argument; the details appear in the proof of Theorem 8.19 of Goldrei on pages 224 – 225 of the latter.

The first crucial observation is that there is a set **U** of well – ordered sets such that if **W** is a well – ordered set supporting a **1 – 1** mapping into **A,** then **W** is in **1 – 1** order – preserving correspondence with some well – ordered set in **U.** To see this, note that every such **W** is in **1 – 1** order – preserving correspondence with a subset of **A** and thus the collection of such subsets with well – orderings is in **1 – 1** correspondence with a subset of the set **P(A) × P(A × A).**

Each well – ordered set corresponds to a unique ordinal number, so let **V** be the set of all ordinal numbers which correspond to the well – ordered sets in **U.** By Theorem 13 above we know that **V** has an upper bound, and of course there are also ordinals which are strictly larger than this upper bound. Every such ordinal fulfills the condition in the conclusion of the theorem, for each such ordinal is greater than all the ordinals that admit **1 – 1** mappings into **A.**■

VII : The Axiom of Choice and related properties

Near the end of Section **VI.4** we listed several basic questions about transfinite cardinal numbers, and we shall restate them here for the sake of convenience:

1. Is the partial ordering of cardinal numbers a linear ordering?
2. Is $\aleph_0$ the smallest transfinite cardinal number?
3. If **A** is an infinite set, does it follow that the idempotent identities $|\mathbf{A}| \cdot |\mathbf{A}| = |\mathbf{A}|$ and $|\mathbf{A}| + |\mathbf{A}| = |\mathbf{A}|$ always hold?
4. If there is a surjection from **A** to **B**, does it follow that $|\mathbf{B}| \leq |\mathbf{A}|$?
5. Given a cardinal number α, is there a unique minimal cardinal number β such that $\beta > \alpha$?

One purpose of this section is to discuss the issues that arise when one studies such questions, and the overall answer may be summarized as follows:

> *If certain valid constructions and operations for subsets of the natural numbers $\mathbb{N}$ can be extended to arbitrary sets, then the answers to the questions stated above (and several others) are all affirmative.*

The good news in this statement is that it generates optimism about finding positive answers to the sorts of questions we have described. However, there is also some bad news. The "valid constructions and operations" for subsets of $\mathbb{N}$ can be described very explicitly, but for arbitrary sets the best we can expect are ***nonconstructive existence principles***. This is particularly well illustrated by the following attempt to prove the answer to the fourth question is yes:

> Suppose that **f** is a surjection from **A** to **B**. Then for each $\mathbf{b} \in \mathbf{B}$ we know that the inverse image $\mathbf{f}^{-1}[\{\mathbf{b}\}]$ is nonempty. For each **b** pick some element $\mathbf{g(b)} \in \mathbf{A}$ in this inverse image. Since **g(b)** lies in $\mathbf{f}^{-1}[\{\mathbf{b}\}]$, it follows that $\mathbf{f(g(b))} = \mathbf{b}$ for all **b** and hence the composite $\mathbf{f} \circ \mathbf{g}$ is the identity on **B**. But now **g** must be $\mathbf{1-1}$ by one of the exercises for Section **VI.3**, and therefore we have $|\mathbf{B}| \leq |\mathbf{A}|$.

There are two important points to notice about this:

1. The ideal of picking an element out of the set has a great deal of intuitive appeal.
2. On the other hand, there is no information on exactly how one should pick an element from the given nonempty subset. — In contrast, if we are dealing with subsets of $\mathbb{N}$ then there is a simple explicit method for making such choices; one simply takes the first element of a given nonempty subset.

Taken together, these suggest that we may need to assume it is possible to pick out "possibly random" elements from nonempty subsets in some unspecified manner. During the first few decades of the 20th century mathematicians studied this question extensively. The first phase of this work produced several logically equivalent versions of the crucial assumption described above, the second shows that the logical

consistence of set theory is not compromised if one makes such assumptions, and the third shows that one has acceptable models for set theory in which such assumptions are true and equally acceptable models in which they are false. Since affirmative answers to the given questions (and others) are convenient for many purposes, most mathematicians are willing to make the sorts of assumptions need to justify the informal argument given above, sometimes reluctantly but generally with few reservations.

We shall begin by motivating and stating three standard ways of formulating the nonconstructive existence principle that arises in connection with the questions above. This is done in Sections 1 and 2, with equivalence proofs in Section 3; a reader who prefers to skip the details of the latter may do so without loss of continuity. Section 4 contains answers to those questions in the list which are not answered in Section 2. The final two sections are commentaries on two related issues. We have noted that assuming the nonconstructive existence principles does not compromise the logical soundness of set theory, and Section 5 explains the situation in a little more detail, and it also discusses the "acceptable models" mentioned above. Finally, Section 6 deals with a question dealing with Cantor's original work: All the specific infinite subsets of the real numbers that arose in his studies either had the same cardinal number as the integers or the real numbers, and Cantor's ***Continuum Hypothesis*** states that there are no cardinal numbers α such that $|\mathbb{N}| < \alpha < |\mathbb{R}|$. It turns out that the formal status of this assumption (and an associated ***Generalized Continuum Hypothesis***) is completely analogous to the nonconstructive existence hypothesis discussed in previous sections.

VII.1 : Nonconstructive existence principles

(Halmos, §§ 15 – 17; Lipschutz, §§ 5.9, 9.1 – 9.4)

We have repeatedly noted that the initial and most important motivation for set theory came from questions about infinite sets. As research on such sets progressed during the late nineteenth and early twentieth century, it eventually became evident that most of the underlying principles involved constructing new sets from old ones and the existence of the set of natural numbers. However, it also became clear that some results in set theory depended upon some nonconstructive existence principles. In particular, when mathematicians attempted to answer questions like 1 – 5 at the beginning of this unit, their arguments used ideas that seemed fairly reasonable but could not be carried out explicitly. In the introduction to this unit, we discussed the role of nonconstructive existence principles in analyzing Question 4. Here we shall begin with a similar analysis of Question 2 from the list. We would like to prove the following result.

Theorem 1. *If* **A** *is an infinite set, then* **A** *has a countably infinite subset and hence we have* $\aleph_0 \leq |\mathbf{A}|$.

It will follow from Theorem 1 that $\aleph_0$ ***is the unique smallest infinite cardinal number.***

In Section V.2 we proved a related fact; namely, if A is countably infinite and **B** is an infinite subset of **A**, then $|\mathbf{B}| = \aleph_0$. One important step in the proof relied on the existence of a well – ordering on the standard countably infinite set $\mathbb{N}$; using the $1 - 1$ correspondence between $\mathbb{N}$ and **A**, it follows that **A** also has a well – ordering if it is countably infinite.

The preceding discussion suggests that ***if an infinite set* A *has a well – ordering, then perhaps one can generalize the previous argument for countably infinite sets* A *to cover other infinite sets as well.*** The idea that every set has a well – ordering originally appeared in Cantor's work; he accepted the statement as true but noted that a convincing argument (or a postulate) was needed. Here is a formal statement:

Well – Ordering Principle. *For every nonempty set* **A**, *there is a* ***well-ordering*** *of* **A** *(recall that this is a linear ordering such that each nonempty subset* **B** *of* **A** *has a least element).*

***Proof that the Well – Ordering Principle implies Theorem* 1.** The basic idea is again the same. One defines a $1 - 1$ function from $\mathbb{N}$ to **A** recursively as follows: Let $\mathbf{f(0)}$ be the first element of **A**, and if $\mathbf{f(x)}$ is defined for $\mathbf{x < n}$ then let $\mathbf{f(n)}$ be the first element not in the set $\mathbf{\{f(0), \ldots, f(n-1)\}}$. Such a first element always exists, for the fact that **A** is infinite implies that $\mathbf{A - \{f(0), \ldots, f(n-1)\}}$ is nonempty.■

In order to illustrate the significance of Theorem 1, we shall use it to prove some generalizations of other results from Sections VI.3 and VI.4.

Theorem 2. *If* **A** *is a countable set and* **B** *is an infinite set, then* $|\mathbf{A}| + |\mathbf{B}| = |\mathbf{B}|$.

Corollary 3 (Dedekind – C. S. Peirce**).** *A set is infinite if and only if it can be put into a* $1 - 1$ *correspondence with a proper subset of itself.*■

***Proof that Theorem* 1 *implies Theorem* 2.** By Theorem 1 we know that **B** contains a countably infinite subset **C**. Let $\mathbf{D = B - C}$. It follows immediately that

$$|\mathbf{B}| = |\mathbf{C}| + |\mathbf{D}| = \aleph_0 + |\mathbf{D}|$$

and therefore we have

$$|\mathbf{A}| + |\mathbf{B}| = |\mathbf{A}| + |\mathbf{C}| + |\mathbf{D}| = |\mathbf{A}| + \aleph_0 + |\mathbf{D}|.$$

The results of Section VI.4 imply that $\aleph_0 = |\mathbf{A}| + \aleph_0$, and if we combine this with the two lines of equations displayed above we conclude that $|\mathbf{A}| + |\mathbf{B}| = |\mathbf{B}|$, as required.■

Here is another important implication of the Well – Ordering Principle for transfinite cardinal numbers. Given the simplicity of the statement and its obvious validity for countable cardinals, it is somewhat surprising that all known proofs use the Well – Ordering Principle or some equivalent statement.

Theorem 4. *If* **A** *and* **B** *are sets, then either* $|\mathbf{A}| \leq |\mathbf{B}|$ *or* $|\mathbf{B}| \leq |\mathbf{A}|$.

Informally, this means that the cardinalities of sets are linearly ordered.

Proof. Choose well – orderings for **A** and **B**. The results of Section **VI.6** then show that either **A** is in order – preserving $\mathbf{1-1}$ correspondence with a subset of **B** or vice versa.■

Although Cantor regarded the Well – Ordering Principle as a "fundamental principle of thought," one disadvantage of assuming this is that the result is difficult to illustrate by means of nontrivial examples. In particular, ***no one has ever constructed a well – ordering of the real numbers***, and most if not all mathematicians find it very difficult to imagine how one might explicitly construct such a relation.

There are many equivalent ways of formulating set – theoretic assumptions that are logically equivalent to the Well – Ordering Principle. Perhaps the most widely used in the development of set theory is the following, which was introduced by E. Zermelo as an "unobjectionable logical principle."

AXIOM OF CHOICE (AC). *If* **A** *is a nonempty set and* $\mathbf{P_+(A)}$ *denotes the set of all nonempty subsets of* **A**, *then there is a function* $\mathbf{f : P_+(A) \to A}$ *such that* $\mathbf{f(B) \in B}$ *for every nonempty subset* $\mathbf{B \subset A}$.

A function of the type described in the conclusion is often called a ***choice function*** on the nonempty subsets of **A**.

Most mathematicians subjectively regard this statement as far more plausible than the Well – Ordering Principle, but as noted below (and in Section 3) ***the two statements are in fact logically equivalent***. Both the Well – Ordering Principle and the Axiom of Choice are nonconstructive existence statements.

The Axiom of Choice is precisely what we need to justify the argument sketched in the introduction to prove the following result:

Theorem 5. *Suppose that* **A** *is a set and* $\mathbf{f : A \to B}$ *is a surjection. Then* $\mathbf{|B| \le |A|}$.

Proof that the Axiom of Choice implies Theorem 5. Once again the basic idea is similar to the corresponding proof in the previous section. Let $\mathbf{g : P_+(A) \to A}$ be a choice function for the nonempty subsets of **A**. Define a function $\mathbf{h : B \to A}$ by the formula.

$$\mathbf{h(b) = g\left(f^{-1}[\{b\}]\right).}$$

Then the choice function condition $\mathbf{h(b) = f^{-1}[\{b\}]}$ implies that $\mathbf{f \circ h(b) = b}$. The theorem will follow if we can show that **h** is a $\mathbf{1-1}$ mapping, and the latter follows because $\mathbf{h(x) = h(y)}$ implies $\mathbf{x = f \circ h(x) = f \circ h(y) = y}$.■

Equivalent statements

For some time there was uncertainty whether the Axiom of Choice, or some equivalent statement, should be included in the axioms for set theory. In an effort to understand the situation more clearly, many statements equivalent to the Axiom of Choice were introduced. Each had its own advantages and disadvantages. The sites listed below give 27 different statements that play a significant role in higher mathematics and are logically equivalent to the axiom of choice:

http://www.math.vanderbilt.edu/~schectex/ccc/excerpts/equivac1.gif

http://www.math.vanderbilt.edu/~schectex/ccc/excerpts/equivac2.gif

A full discussion of these equivalent statements is beyond the scope of these notes, but we shall mention one particularly important and frequently used example.

"Zorn's Lemma." *If* **A** *is a partially ordered set in which linearly ordered subsets have upper bounds, then* **A** *has a maximal element.*

Zorn's lemma was first discovered by K. Kuratowski (1896 – 1980) and independently a decade later by M. Zorn (1906 – 1993); it is also sometimes known as the Kuratowski – Zorn Lemma. This statement is arguably the most useful of all the statements that are logically equivalent to the Axiom of Choice for reasons to be discussed in Section 2.

Issues for further consideration

There are several points that arise naturally in connection with the three nonconstructive existence statements (the Well – Ordering Principle, the Axiom of Choice and Zorn's Lemma) that we have formulated.

1. How does one show that the three nonconstructive existence principles are logically equivalent?
2. Is there a simple example to illustrate the uses of Zorn's Lemma?
3. What sorts of logical problems, if any, arise if one assumes the three statements we have introduced?
4. To what extent are mathematicians willing to accept these statements?

We shall address the first question in Section 3 and the second in Section 2. A detailed discussion of the last two questions appears in Section 5, but for the time being we note that any logical problems that might exist in set theory are present regardless of whether or not one assumes the three nonconstructive existence statements we have introduced in this section; if logical difficulties exist under the assumption of these statements, then by results of K. Gödel there are already logical difficulties even if one does not make these assumptions. Also, the general (but not unanimous) acceptance of such statements in present day mathematics is reflected by our extensive discussion of them in these notes.

VII.2 : Extending partial orderings

(Lipschutz, § 7.6)

In the previous section we made no attempt to motivate Zorn's Lemma, but we shall try to do so here with an example illustrating its use in mathematics. The following type of problem is standard in discrete mathematics courses:

Problem. *Suppose that* **A** *is a finite set, and let* $P \subset A \times A$ *be a partial ordering. Is there a linear ordering* $Q \subset A \times A$ *such that* $P \subset Q$**?**

The existence of such linear orderings is important for practical purposes**.** Suppose one has a list of things to be completed that we shall call **A,** with requirements that certain items on the list must be finished before others**.** These requirements correspond to a partial ordering P of the items on the list, and finding a linear ordering Q containing P then puts the items into a linear sequence in which they can be completed**.** An example is described in one of the exercises for this section**.**

It turns out that one can always find a linear ordering Q which solves the problem stated above, and this is essentially worked out in Lipschutz using equivalent language (the concept is called ***consistent enumeration*** in Lipschutz)**.** Specifically**,** given a partial ordering P on a finite set **A** with **n** elements**,** Theorem **7.1** on page 172 of Lipschutz proves the existence of a strictly increasing function **f** the set **A** to the standard example $\{1, \ldots, n\}$**;** the proof is given in Problem **7.17** on page 187 (also see pages 195 – 196)**.** If we define a binary relation Q on **A** by the rule $x \, Q \, y$ if and only if $f(x) \leq f(y)$**,** then it is a routine exercise to check that Q is a linear ordering which contains P**.**

We shall use Zorn's Lemma to prove that one can find similar linear orderings even if the set **A** is not finite**.**

Theorem 1. *Let* **A** *be a set, and let* $P \subset A \times A$ *be a partial ordering. Then there is a linear ordering* $Q \subset A \times A$ *such that* $P \subset Q$**.**

We frequently say that Q is a ***compatible linear ordering*** or Q *is compatible with* P**.**

As noted above, a result of this type is useful for many purposes. For example, if **X** is a finite set and **A** is a family of subsets of **X,** then sometimes one wants prove a fact about the elements of **A** by mathematical induction, where **A** is linearly ordered such that for each pair of elements **B, C** in **A** such that $B \subset C$ we also have $B < C$**.**

The nonconstructive nature of Theorem 1 is illustrated by one simple fact**:** A compatible linear ordering for the set $\mathbf{P}(\mathbb{N})$ of subsets of the natural numbers (ordered by inclusion) has not been explicitly constructed**.** In contrast**,** given an arbitrary partial ordering on a finite set**,** one can use the proof in Lipschutz to construct an explicit compatible linear ordering**.**

***Proof of Theorem* 1. (**)** We follow the approach outlined above**,** first showing that there is a maximal partial ordering containing the given one and then showing that such a maximal partial ordering must be a linear ordering**.**

Let **C** be the collection of all partial orderings of **A** that contain P**.** Then **C** is partially ordered by set – theoretic inclusion**.** Let **D** be a subset of **C** that is linearly ordered by inclusion**.** If we can show that **D** has an upper bound in **C,** then Zorn's Lemma will imply that **C** has a maximal element**.**

Denote the elements of **D** by Q_x where **x** runs through some indexing set **X,** and let Q be the union of all the sets Q_x**.** Clearly Q contains P since each Q_x does**;** we would like to show that Q is also a partial ordering**.** The relation Q is reflexive because Q contains P and P is reflexive**.** To verify the relation Q is asymmetric**,** suppose that both **(a, b)** and

(b, a) belong to ***Q*****.** Then there are partial orderings Q_x and Q_y such that **(a, b)** belongs to Q_x and **(b, a)** belongs to Q_y**.** Since **D** is linearly ordered by inclusion it follows that one of Q_x and Q_y contains the other**.** If Q_z is the larger relation**,** then both **(a, b)** and **(b, a)** belong to Q_z**,** and since the latter is a partial ordering this means that $a = b$**.** Finally**,** suppose that both **(a, b)** and **(b, c)** belong to ***Q*****.** Then there are partial orderings Q_x and Q_y such that **(a, b)** belongs to Q_x and **(b, c)** belongs to Q_y**.** Since **D** is linearly ordered by inclusion it follows that one of Q_x and Q_y contains the other**.** If Q_z is the larger relation, then both **(a, b)** and **(b, c)** belong to Q_y**,** and since the latter is a partial ordering this means that **(a, c)** belongs to Q_z**,** which is contained in ***Q*****.** Therefore ***Q*** is a partial ordering**.** By construction**,** it is an upper bound for the elements of **D,** and thus Zorn's lemma implies that **C** must have a maximal element**.**■

The second part of the proof of the theorem is contained in the following result**.**

Proposition 2. *Let* **A** *be a set, and let* $P \subset A \times A$ *be a maximal partial ordering. Then* ***P*** *is a linear ordering***.**

Proof. **(***)** Suppose that ***P*** is not a linear ordering**.** Then we can find **x, y** in **A** such that neither **(x, y)** nor **(y, x)** lies in ***P*****.** We shall obtain a contradiction by expanding ***P*** to a partial ordering that contains **(x, y).** In order to express the argument in familiar notation we shall write $u \leq_P v$ to signify that **(u, v)** lies in ***P*****.**

Define a new binary relation ***Q*** such that **(u, v)** lies in ***Q*** if and only if either $u \leq_P v$ or else both $u \leq_P x$ and $y \leq_P v$**.** The proof of the proposition then reduces to showing that ***Q*** is a partial ordering**.**

*The relation **Q** is reflexive.* Since ***P*** is a partial ordering, for each $a \in A$ we know that $(a, a) \in P \subset Q$**.**

*The relation **Q** is transitive.* Suppose that $(a, b) \in Q$ and $(b, c) \in Q$**.** Then there are two options for each of the ordered pairs in the preceding sentence and thus a total of four separate cases to consider**:**

1. We have $a \leq_P b$ together with $b \leq_P c$**.**
2. We have $a \leq_P b$ together with both $b \leq_P x$ and $y \leq_P c$**.**
3. We have both $a \leq_P x$ and $y \leq_P b$ together with $b \leq_P c$**.**
4. We have both $a \leq_P x$ and $y \leq_P b$ together with both $b \leq_P x$ and $y \leq_P c$**.**

In the first case**,** since ***P*** is a partial ordering we have $a \leq_P c$**,** so that $(a, c) \in Q$**.** In the second case**,** since ***P*** is a partial ordering we have $a \leq_P x$**,** and therefore **(a, c)** satisfies the second criterion to be an element of ***Q*****.** In the third case**,** since ***P*** is a partial ordering we have $y \leq_P c$**,** and therefore **(a, c)** satisfies the second criterion to be an element of ***Q*****.** Finally**,** in the fourth case since ***P*** is a partial ordering the middle two conditions imply that $y \leq_P x$**,** which contradicts our original hypothesis that neither of the relations $x \leq_P y$ or $y \leq_P x$ is valid**.** Therefore the fourth case is impossible**,** and this completes the proof of transitivity**.**

*The relation **Q** is antisymmetric.* Suppose that $(a, b) \in Q$ and $(b, a) \in Q$. Then we have the same four cases as in the proof of transitivity, the only difference being that one must replace **c** by **a** in each case. In the first case, since ***P*** is a partial ordering we must have $a = b$. In all the remaining cases, since ***P*** is a partial ordering the given conditions combine to imply $y \leq_P x$, which contradicts the assumption on ***Q***. Thus only the first case is possible, and this completes the proof that the relation ***Q*** is antisymmetric.■

As noted in Section 1, for many decades mathematicians have generally found Zorn's Lemma to be particulary effective for proving theorems that depend upon the Axiom of Choice, partly because most of these results translate easily into the existence of a maximal object of some sort. From this perspective, the proofs usually have two distinct parts:

1. Showing that a maximal object of some type must exist using Zorn's Lemma.
2. Showing that such maximal objects must have certain desired properties.

Here is another application of Zorn's Lemma to partially ordered sets; as indicated by the name, this statement was formulated by F. Hausdorff (1868 – 1942) and in fact was known before Zorn's Lemma was discovered.

Theorem 3 (Hausdorff Maximal Principle**).** *Every nonempty partially ordered set contains a maximal linearly ordered subset.*

Proof. Let **X** be the nonempty partially ordered set, let ***R*** be the partial ordering, and consider the family **Y** of all subsets **A** of **X** such that

$$R|A = R \cap A \times A$$

Is a linear ordering on **A**, with the partial ordering of **Y** given by set – theoretic inclusion. The family **Y** is nonempty, for if $x \in X$ then one has the trivial linear ordering

$$\{x\}\times\{x\} = R \cap (\{x\}\times\{x\})$$

on the one point subset $\{x\} \subset X$.

Suppose that we have a linearly ordered subfamily of subsets X_a as above. If we take $W = \cup_a X_a$ then we claim that $T = R|W$ is a linear ordering on **W**. By construction it is a partial ordering, so the only point to prove is the dichotomy property. Suppose now that $x, y \in W$. Then one can find **a** and **b** such that $x \in X_a$ and $y \in X_b$. The linear ordering property implies that one of **a** or **b** is greater than or equal to the other; if **c** denotes this element, then we have $x, y \in X_c$. Since the latter set is linearly ordered with respect to

$$S_c = R|X_c$$

it follows that either $(x, y) \in S_c$ or $(y, x) \in S_c$, and since the latter is contained in ***T*** it follows that one of the two pairs must lie in ***T***. Therefore ***T*** is a linear ordering, and therefore **W** is an upper bound in **Y** for all of the linearly ordered subsets X_a.

We can now use Zorn's Lemma to conclude that **Y** has a maximal element, which is given by a subset **M** with the linear ordering $L = R|M$. It follows immediately that **M** is a maximal linearly ordered subset.■

For the sake of completeness we note that ***the Hausdorff Maximal Principle is also logically equivalent to Zorn's Lemma*** (or the Axiom of Choice or the Well – Ordering Principle).

VII.3 : Equivalence proofs

(Halmos, §§ 15 – 20; Lipschutz, §§ 5.9, 9.1 – 9.5, 9.7)

> [From a purely intuitive viewpoint, it appears that] the Axiom of Choice is obviously true, the well-ordering principle [is] obviously false, and who can tell about Zorn's lemma?
>
> J. Bona (1945 –)

Although the Axiom of Choice, the Well – Ordering Principle and Zorn's Lemma are logically equivalent, most mathematicians do not view them as equally easy to accept as assumptions. As indicated in the quotation, the Axiom of Choice seems intuitively easier to believe than the others, while the Well – Ordering Principle is often seen as counter – intuitive and Zorn's Lemma is viewed as too complex for any intuition. Therefore, proofs that these three statements are logically equivalent are not only needed for the sake of logical completeness, for they also provide reassurance that the less intuitive statements are equally valid. The purpose of this section is to give (or at least sketch) the proofs that the three basic statements are logically equivalent. This material will not be used in later sections and may be skipped without loss of continuity. At some points we shall need properties of well – ordered sets that were stated without full proofs in Section **VI.6.**

Proving that the Well – Ordering Principle implies the Axiom of Choice. This is the simplest of all the arguments: Let **A** be a nonempty set, suppose we are give a well – ordering, and let $\mathbf{P_+(A)}$ denote the set of all nonempty subsets of **A.** Define a function $\mathbf{f : P_+(A) \to A}$ such that for every nonempty subset $\mathbf{B \subset A}$, the image **f(B)** is equal to the ***unique minimal element*** of **B** with respect to the well – ordering. Then by construction we always have $\mathbf{f(B) \in B}$.■

Proving that the Axiom of Choice implies the Well – Ordering Principle. **(****)** A fully rigorous proof requires many of the results on ordinals from the previous section as well as a strong version of transfinite recursion. In many ways this is the most difficult implication to prove, so we shall merely outline the argument here.

Let **X** be a set, and let $k: P_+(X) \to X$ be a choice function. By Hartogs' Theorem there is an ordinal λ such that there is no $1-1$ mapping from λ to **X**. Define $f: \lambda \to X \cup \{X\}$ recursively as indicated below for a given $\alpha \in \lambda$; there are two cases depending upon whether or not the set $J_\alpha = f[[0, \alpha)]$ is a proper subset of **X**.

1. If J_α is a proper subset of **X**, take $f(\alpha) = k(X - J_\alpha)$.
2. If J_α is not a proper subset of **X**, take $f(\alpha) = X$.

By construction, if $f(\alpha) \in X$, then the restriction of **f** to the closed interval $[0, \alpha]$ is $1-1$. Furthermore, **f** is $1-1$ on the inverse image of **X**.

By the choice of λ, we know there is a $\gamma \in \lambda$ such that $f \mid [0, \gamma]$ is not $1-1$; let β be the least such ordinal. It then follows that **f** is $1-1$ on $[0, \beta)$ and $f(\gamma) = X$ for $\gamma \geq \beta$. Furthermore, it also follows that **f** defines a $1-1$ from $[0, \beta)$ to **X**.■

Proving that the Axiom of Choice and the Well – Ordering Principle imply Zorn'sLemma. (**) If Zorn's Lemma is false, then there exists a partially ordered set **X** such that every linearly ordered subset has an upper bound, and for each element **u** of **X** it is possible to find a larger element **v**.

Using Hartogs' Theorem we can find an ordinal λ such that there is no $1-1$ mapping from λ to **X**; alternatively, we can find λ by taking a well – ordering of the power set **P(X)**. We claim it is possible to define a strictly increasing map **f** from λ to **X** by transfinite recursion. If we can do this, we shall have a contradiction because there is no $1-1$ map from λ to **X**. Let $k: X \to P(X)$ be a choice function.

Define $f(0_X) = k(X)$ to begin the process. Suppose now that we have defined the function on $[0, \alpha)$, and let $J_\alpha = f[[0, \alpha)]$. By hypothesis the latter is a linearly ordered subset of **X** and as such it has an upper bound. Use the choice function **k** to select a particular upper bound $u(\alpha)$. We are also assuming that **X** has no maximal element so the set of all elements strictly greater than $u(\alpha)$ is nonempty; use the choice function **k** again to select some $f(\alpha) > u(\alpha)$. Since **f** is strictly increasing for $\beta < \alpha$ and $f(\alpha)$ is greater than every element of J_α by construction, it follows that **f** is $1-1$ on the closed interval $[0, \alpha]$. This completes the recursive step in the definition of the strictly increasing map $f: \lambda \to X$.

As noted in the second paragraph of the argument, this yields a contradiction. Where is the problem? The construction of **f** relies heavily on the fact that **X** has no maximal element, so this must be false. Thus **X** must have a maximal element, and the existence of such an element is exactly what is needed to prove Zorn's Lemma.■

Proving that Zorn's Lemma implies the Well – Ordering Principle. (**) This is a typical example of how Zorn's Lemma is used in mathematics. General comments on this were given in Section 2, so our discussion here will be very brief. The idea is to start with a set **X** and to consider an auxiliary partially ordered set **W** of well – orderings, with $\alpha \leq \beta$ if and only if α corresponds to an initial segment of β. Then one shows that **W** satisfies the hypotheses of Zorn's Lemma and hence has a maximal element. The final step is to check that this maximal element is a well – ordering for the entire set **X**.■

Here are some online references for more information about the Axiom of Choice and related topics:

http://en.wikipedia.org/wiki/Axiom_of_choice

http://www.math.vanderbilt.edu/~schectex/ccc/choice.html

http://planetmath.org/encyclopedia/MultiplicativeAxiom.html

VII.4: Additional consequences

(Halmos, § 15; Lipschutz, §§ 9.1, 9.7)

In this section we shall complete the discussion of the questions about cardinal numbers that were raised at the beginning of this unit, and we shall also discuss a few other basic mathematical facts which logically depend upon the Axiom of Choice or an equivalent statement. Many other examples arise in virtually all basic graduate level mathematics courses.

Some of the preceding online references contain thorough, but not overwhelming, summaries of basic mathematical results whose proofs require the Axiom of Choice. In this subsection we shall restrict attention to a few that involve material from lower level undergraduate courses in the mathematical sciences or topics previously covered in this course.

The first simple result is essentially a restatement of the definition of a general Cartesian product; in fact, the conclusion of the theorem is the version of the Axiom of Choice stated on page 59 of Halmos, and therefore the theorem implies that our version is equivalent to the version in Halmos.

Theorem 1. (Nontriviality Principle for Products.) *If the Axiom of Choice is true, then a product of any nonempty family $\mathcal{F}$ of nonempty sets is nonempty (we assume that the elements of $\mathcal{F}$ indexed by $\mathcal{F}$ itself).*

Proof. Given a family $\mathcal{F}$ of sets a choice function defines an element of the product

$$\prod \{B \mid B \in \mathcal{F}\}.$$

In fact, the converse is also true, for a choice function corresponds to an element of the Cartesian product displayed above.■

Consequences for transfinite cardinal numbers

Zorn's Lemma also provides a particularly effective means for proving the following basic property of transfinite cardinals which generalizes an earlier result (Theorem **VI.4.8**) for the first infinite cardinal number $\aleph_0$:

Theorem 2 (Idempotent Laws for transfinite cardinals**).** *If* **A** *is an infinite set, then we have* $|\mathbf{A}| + |\mathbf{A}| = |\mathbf{A}|$ *and* $|\mathbf{A}| \cdot |\mathbf{A}| = |\mathbf{A}|$.

Corollary 3. *If* **A** *and* **B** *are nonempty sets and at least one is infinite, then*

$$|\mathbf{A}| + |\mathbf{B}| = |\mathbf{A}| \cdot |\mathbf{B}| = |\mathbf{C}|$$

where $|\mathbf{C}|$ *is the larger of* $|\mathbf{A}|$ *and* $|\mathbf{B}|$.

The final portion of this statement relies on the fact that cardinal numbers are linearly ordered, which was established in Theorem **VII.2.4** above. Of course, the corollary is generally (in fact, almost always) false if both **A** and **B** are finite.

Proof that Theorem 2 implies Corollary 3. Without loss of generality, *we might as well assume that* $|\mathbf{A}|$ *is the larger of the two cardinal numbers*. If we can prove the result in this case, the proof when $|\mathbf{B}|$ is the larger will follow by interchanging the roles of **A** and **B** systematically throughout the argument. Such "without loss of generality" reductions are used frequently in mathematical proofs to simplify the discussion.

Since we are assuming $|\mathbf{A}| \geq |\mathbf{B}|$, we may combine the conclusion of Theorem 2 with the basic formal properties of cardinal addition and multiplication to conclude that

$$|\mathbf{A}| \leq |\mathbf{A}| + |\mathbf{B}| \leq |\mathbf{A}| + |\mathbf{A}| = |\mathbf{A}|$$

so that $|\mathbf{A}| + |\mathbf{A}| = |\mathbf{A}|$, and similarly

$$|\mathbf{A}| \leq |\mathbf{A}| \cdot |\mathbf{B}| \leq |\mathbf{A}| \cdot |\mathbf{A}| = |\mathbf{A}|$$

so that $|\mathbf{A}| \cdot |\mathbf{B}| = |\mathbf{A}|$.■

Proof of Theorem 2. We begin with the additive identity, both because it is simpler and because it is needed to prove the multiplicative identity. Both arguments are based upon Zorn's Lemma.

Proof that $|\mathbf{A}| + |\mathbf{A}| = |\mathbf{A}|$. — Let $\mathbf{U_A}$ be the set of all pairs **(B, f)** where $\mathbf{B} \subset \mathbf{A}$ is a nonempty subset and $\mathbf{f} : \mathbf{B} \amalg \mathbf{B} \to \mathbf{B}$ is a $1 - 1$ correspondence. If we define **(B, f)** $\leq$ **(C, g)** to be true if and only if $\mathbf{g(b, n)} = \mathbf{f(b, n)}$ for $\mathbf{n} = 1$ or 2, then routine calculations show that $\leq$ defines a partial ordering on $\mathbf{U_A}$.

The set $\mathbf{U_A}$ is nonempty because **A** contains a countably infinite subset **C**, and by Theorem **VI.4.8** there is a bijection from $\mathbf{C} \amalg \mathbf{C}$ to **C**.

Suppose now that we have a linearly ordered subset of $\mathbf{U_A}$ whose elements have the form $(\mathbf{B_t}, \mathbf{f_t})$, where **t** lies in some indexing set. For each **t** let $\mathbf{G_t}$ denote the graph of **t**, let **B** be the union of the sets $\mathbf{B_t}$, and let **G** be the union of the graphs $\mathbf{G_t}$. We claim that **G** is the graph of a bijection from $\mathbf{B} \amalg \mathbf{B}$ to **B**. If so, then $(\mathbf{B}, \mathbf{f}) \geq (\mathbf{B_t}, \mathbf{f_t})$ for all **t** and hence the hypotheses of Zorn's Lemma apply.

Suppose that $\mathbf{z} \in \mathbf{B}$, and choose **t** such that $\mathbf{z} \in \mathbf{B_t}$. Then there is a uniqute $\mathbf{w} \in \mathbf{B_t}$ such that $(\mathbf{z}, \mathbf{w}) \in \mathbf{G_t}$; we claim there are no other points in **G** with first coordinate equal to **z**. If $(\mathbf{z}, \mathbf{x}) \in \mathbf{G}$, then there is some s such that $(\mathbf{z}, \mathbf{x}) \in \mathbf{G_s}$. Choose **r** so that $\mathbf{G_r}$ is the larger of $\mathbf{G_s}$ and $\mathbf{G_t}$; then $(\mathbf{z}, \mathbf{w})$ and $(\mathbf{z}, \mathbf{x}) \in \mathbf{G_r}$ imply $\mathbf{w} = \mathbf{x}$ because $\mathbf{G_r}$ is

the graph of a function. Thus **G** is the graph of a function. What is the domain of **G?** If $(z, w) \in G$, then $z \in B_t \amalg B_t \subset B \amalg B$ for some **t,** and conversely if $z \in B \amalg B$ then for some **t** we have $z \in B_t \amalg B_t$, and consequently there is an ordered pair of the form $(z, w) \in G_t \subset G$.

Next, we need to show that the function **f** with graph **G** is a bijection. If $f(x) = f(y)$ then as before one can find a single set **t** such that $x, y \in B_t \subset B \amalg B$ for this choice of **t,** and conversely if $z \in B \amalg B$ then for some **t** we have $z \in B_t \amalg B_t$. Then we have

$$f_t(x) = f(x) = f(y) = f_t(y)$$

and since f_t is $1-1$ it follows that $x = y$. Also, if $z \in B$, choose **t** such that $z \in B_t$, so that $z = f_t(w) = f(w)$ for some **w** and hence **f** is onto. This completes the proof that linearly ordered subsets of U_A have maximal elements.

By Zorn's Lemma there is a maximal element (M, h) of U_A, and by construction we have $|M| + |M| = |M|$. If $|M| = |A|$ then the proof is complete, so assume the cardinalities are unequal. Since **M** is a subset of **A** we must have $|M| < |A|$, and in fact by Theorem VII.1.2 it follows that $|A - M|$ must be infinite (if it were finite then we would have $|M| = |A|$). Let $C \subset M$ be a countably infinite set, let $h_0 : C \amalg C \to C$ be a bijection, and consider the map

$$k : (M \cup C) \amalg (M \cup C) \to M \cup C$$

defined as the composite

$$(M \cup C) \amalg (M \cup C) = (M \amalg M) \cup (C \amalg C) \to M \cup C$$

sending $x \in M \amalg M$ to $h(x)$ and $y \in C \amalg C$ to $h_0(x)$. It follows immediately that the element $(M \amalg C, k)$ is strictly greater than (M, h), contradicting the maximilaity of the latter. The problem arises from our assumption that $|M|$ and $|A|$ are unequal, and thus we have $|M| = |A|$ and we have proved the statement about $|A| + |A|$.

Proof that $|A| \cdot |A| = |A|$. — Let V_A be the set of all pairs (B, f) where $B \subset A$ is a nonempty subset and $f : B \times B \to B$ is a $1-1$ correspondence (bijection). If we now set $(B, f) \leq (C, g)$ if and only if $g(b_1, b_2) = f(b_1, b_2)$ for $b_1, b_2 \in B$, then once again routine calculations show that $\leq$ defines a partial ordering on V_A.

The set V_A is nonempty because **A** contains a countably infinite subset **C,** and by Theorem VI.4.8 there is a bijection from $C \times C$ to **C.**

Suppose now that we have a linearly ordered subset of V_A whose elements have the form (B_t, f_t), where **t** lies in some indexing set. The argument in the previous part of the proof extends to show that this linearly ordered set has an upper bound, whose graph is again the union of the graphs of the functions f_t. Therefore, once again Zorn's Lemma implies the existence of a maximal element (M, h) and once again the conclusion is true if $|M| = |A|$, so suppose the latter is false. It follows that $|M| < |A|$. We can now use the first part of the theorem to conclude that $|M| + |M| = |M|$, and if we combine this with the equation $|M| + |A - M| = |A|$ we conclude that $|M| < |A - M|$. In fact, the first part of the theorem implies that $|M| = 3|M|$ and consequently we have $3|M| < |A - M|$.

The inequality $|\mathbf{M}| < |\mathbf{A} - \mathbf{M}|$ implies the existence of a subset $\mathbf{N} \subset \mathbf{A} - \mathbf{M}$ such that $|\mathbf{N}| = |\mathbf{M}|$, and in fact the last sentence of the previous paragraph implies that we may write **N** as a union of pairwise disjoint subsets $\mathbf{N_1}, \mathbf{N_2}, \mathbf{N_3}$ which have the same cardinality as **M** and **N.** Define an extension of $\mathbf{h}: \mathbf{M} \times \mathbf{M} \to \mathbf{M}$ to

$$\mathbf{k}: (\mathbf{M} \cup \mathbf{N}) \times (\mathbf{M} \cup \mathbf{N}) \to \mathbf{M} \cup \mathbf{N}$$

using the following breakdown by cases:

(1) On $\mathbf{M} \times \mathbf{M}$, **k** is given by **h.**

(2) On $\mathbf{M} \times \mathbf{N}$, **k** is given by $\mathbf{M} \times \mathbf{N} \leftrightarrow \mathbf{N} \times \mathbf{N} \leftrightarrow \mathbf{M} \times \mathbf{M} \leftrightarrow \mathbf{M} \leftrightarrow \mathbf{N_1}$, where the $\mathbf{1-1}$ correspondences are determined by the standard correspondences $\mathbf{M} \leftrightarrow \mathbf{N}$, $\mathbf{N} \leftrightarrow \mathbf{N_1}$, and $\mathbf{M} \times \mathbf{M} \leftrightarrow \mathbf{M}$.

(3) On $\mathbf{N} \times \mathbf{M}$, **k** is given by $\mathbf{N} \times \mathbf{M} \leftrightarrow \mathbf{N} \times \mathbf{N} \leftrightarrow \mathbf{M} \times \mathbf{M} \leftrightarrow \mathbf{M} \leftrightarrow \mathbf{N_2}$, where the $\mathbf{1-1}$ correspondences are determined by the standard correspondences $\mathbf{M} \leftrightarrow \mathbf{N}$, $\mathbf{N} \leftrightarrow \mathbf{N_2}$, and $\mathbf{M} \times \mathbf{M} \leftrightarrow \mathbf{M}$.

(4) On $\mathbf{N} \times \mathbf{N}$, **k** is given by $\mathbf{N} \times \mathbf{N} \leftrightarrow \mathbf{M} \times \mathbf{M} \leftrightarrow \mathbf{M} \leftrightarrow \mathbf{N_3}$, where the $\mathbf{1-1}$ correspondences are determined by the standard correspondences $\mathbf{M} \leftrightarrow \mathbf{N}$, $\mathbf{N} \leftrightarrow \mathbf{N_3}$, and $\mathbf{M} \times \mathbf{M} \leftrightarrow \mathbf{M}$.

By construction $(\mathbf{M} \cup \mathbf{N}, \mathbf{k})$ is strictly greater than $(\mathbf{M}, \mathbf{h})$, contradicting the maximilaity of the latter. The problem arises from our assumption that $|\mathbf{M}|$ and $|\mathbf{A}|$ are unequal, and thus we have $|\mathbf{M}| = |\mathbf{A}|$, verifying the statement of the theorem about $|\mathbf{A}| \cdot |\mathbf{A}|$.■

The following consequence of Theorem 2 and Corollary 3 is useful in many situations.

Proposition 4. *Let* $\{\mathbf{A_n}\}$ *be a countable sequence of infinite sets such that* $|\mathbf{A_n}| \leq \alpha$ *for all* **n** *and there is some nonnegative integer* **M** *such that* $|\mathbf{A_M}| = \alpha$. *Then we have* $|\bigcup_{\mathbf{n}} \mathbf{A_n}| = \alpha$.

Proof. Let **B** denote the union. Then we clearly have $\alpha \leq |\mathbf{B}|$ since $|\mathbf{A_M}| = |\mathbf{B_M}|$ for some $\mathbf{B_M} \subset \mathbf{B}$. On the other hand, by the cardinality assumption we also have injections $\mathbf{f_n}: \mathbf{A_n} \to \mathbf{A_M}$ for all **n,** and we can piece these together to obtain an injection

$$\varphi: \coprod_{\mathbf{n}} \mathbf{A_n} \to \mathbb{N} \times \mathbf{A_M}$$

defined by the formula $\varphi(\mathbf{n}, \mathbf{x}) = \big(\mathbf{n}, \mathbf{f_n}(\mathbf{x})\big)$. There is also a surjection

$$\psi: \coprod_{\mathbf{n}} \mathbf{A_n} \to \mathbf{B}$$

sending $\{\mathbf{n}\} \times \mathbf{A_n}$ bijectively to $\mathbf{A_n} \subset \mathbf{B}$. If we now apply Exercise **VII.1.2,** it follows that $|\mathbf{B}| \leq \aleph_0 \times \alpha$, and by Corollary 3 the right hand side is equal to α. We can now use the Schröder – Bernstein Theorem to conclude that $|\mathbf{B}| = \alpha$.■

Corollary 5. *In the setting of the previous result, if* $|\mathbf{A_n}| = \alpha$ *for all* **n,** *then* $|\mathbf{B}| = \alpha$.■

Zorn's Lemma in algebra

Several other applications of Zorn's Lemma to basic questions in algebra are worked out on page 226 of Lipschutz (in particular, see Problems 9.6 and 9.7); for example, Problem 9.6 uses Zorn's Lemma to prove that ***every infinite – dimensional vector space has a basis.***

A formal definition of cardinal numbers

We can use the Well – Ordering Principle to give a simple and mathematically sound definition of cardinal numbers. The key to doing so is contained in the following result:

Proposition 6. *Let* $\mathbf{X}$ *be a set, and let* $\mathbf{C_X}$ *be the collection of ordinal numbers* α *for which there is a* $\mathbf{1-1}$ *mapping from* α *into* $\mathbf{X}$. *Then* $\mathbf{C_X}$ *is a nonempty set.*

Definition. The least element of $\mathbf{C_X}$ is called the ***cardinal number*** of $\mathbf{X}$. From this perspective we may view $\aleph_0$ as being equal to the first infinite ordinal, which is ω.

Proof. The class $\mathbf{C_X}$ is nonempty by the well – ordering principle. To show it is a set, it suffices to prove that there is some ordinal number β for which there is ***no*** $\mathbf{1-1}$ mapping from β into $\mathbf{X}$. It then follows that $\alpha < \beta$ for all $\alpha \in \mathbf{C_X}$, which implies that $\mathbf{C_X}$ is a set. There are two ways of doing this; either one can use Hartogs' Theorem or else one can take the ordinal number associated to a well – ordered set $\mathbf{Y}$ such that $|\mathbf{Y}| = |\mathbf{P(X)}|$; the latter is quicker and perhaps more convincing, but the former is logically more direct. ■

Corollary 7. *The class of cardinal numbers is well – ordered by the restriction of the ordering relation on the ordinal numbers. In particular, given any cardinal number* α *there is a least cardinal number* β *such that* $\beta > \alpha$ *(i.e., there is a* ***next largest cardinal number*** *— this statement was first formulated by Cantor).* ■

In fact, one can say more. Using a suitably strong version of transfinite recursion one can define a strictly order – preserving $\mathbf{1-1}$ correspondence from the ordinal numbers to the infinite cardinal numbers. We have already denoted the first infinite cardinal by $\aleph_0$. Following Cantor's notation, it is customary to denote the next infinite cardinal, which is the image of $\mathbf{1}$ under the recursively defined mapping, by $\aleph_1$. More generally, the cardinal number which corresponds to the ordinal α is denoted by $\aleph_\alpha$.

VII.5: Logical consistency and acceptance

(Halmos, § 15; Lipschutz, §§ 9.1, 9.7)

Whenever it appears that one statement about a mathematical system cannot be derived as a mathematical consequence of the others, there are immediate questions

whether this statement can or should be taken as an additional assumption, and thus near the beginning of the 20th century there were immediate questions about whether the Axiom of Choice or an equivalent statement should be added to the basic assumptions of set theory. Concern over the desirability of adding the Axiom of Choice or an equivalent statement to the axioms for set theory increased with the discovery of difficulties such as Russell's Paradox. Most of these difficulties were resolved within two decades by a careful foundation of the axioms for set theory, but it was still not known if adding the Axiom of Choice might still lead to a logical contradiction. We shall discuss subsequent developments about logical consistency later in this section.

As noted earlier, this section discusses some conceptual points about the following basic questions:

1. Does the inclusion of the Axiom of Choice (or an equivalent statement) lead to any further problems?
2. Should the Axiom of Choice (or an equivalent statement) be assumed as an axiom for set theory?

The following additional question will be addressed in the next section.

3. Are there other set – theoretic statements that also should be included as axioms?

We have already noted that Cantor and his contemporaries recognized that something like the Axiom of Choice might have to be taken as an assumption if it could not be proved. Concern over the desirability of adding the Axiom of Choice to the axioms for set theory increased with the discovery of difficulties such as Russell's Paradox near the beginning of the 20th century. Although most of these potential paradoxes in set theory were resolved by a careful foundation of the axioms for the subject, such work did not determine whether the Axiom of Choice and its equivalent statements led to logical consistency problems; in other words, it was still not known if adding the Axiom of Choice or an equivalent statement might eventually lead to a logical contradiction. We shall discuss subsequent developments about logical consistency later in this section; historically, the next development raised further questions about assuming statements like the Axiom of Choice.

The Banach – Tarski Paradox

A new reason for concern about the Axiom of Choice was discovered in the 1920s. The so-called ***Banach – Tarski paradox*** showed that the Axiom of Choice had some extremely strong consequences which seemed to contradict common sense. These raised additional questions about whether the Axiom of Choice should be included in the axioms for set theory. In its original form, the relevant result of S. Banach (1892 – 1945) and A. Tarski (1902 – 1983) states that **if the Axiom of Choice is assumed, then it is possible to take a solid ball in 3 – dimensional space, cut it up into finitely many pieces, and moving them — using only rotation and translation — reassemble the pieces into two balls having the same size as the original one!!**

Such a bizarre result raises serious questions whether one could prove even more results and perhaps even use the Axiom of Choice to obtain a logical contradiction. In particular, at first glance the Banach – Tarski result may seem to violate the basic laws of physics (*e.g.*, Conservation of Matter). Fortunately, this does not reflect a problem with the underlying mathematics, for it is important to note that *the sets in question are*

mathematical *rather than* **physical** *objects*. In particular, there is no meaningful way to define the volumes of the individual pieces, and it is impossible to carry out the construction physically because if one does cut the solid ball into pieces physically (say with a knife or saw), then each piece will have a specific volume (physically, one can find the volumes by sticking the pieces into a large cylinder which contains enough water or other fluid that will not dissolve the pieces). However, even though the Banach – Tarski paradox does not yield a logical contradiction to the axioms of set theory or the fundamental laws of experimental physics, it does raise two fundamental questions:

1. If set theory with the Axiom of Choice yields bizarre conclusions like the existence of the sets described above, is it possible that further work will lead to a contradiction?
2. Is it worthwhile to consider such objects, and if not is it appropriate to have an axiomatic system for set theory that will imply the existence of such physically unreal entities?

One way of answering the second question is that the Axiom of Choice also implies the existence of many things that mathematicians do want for a variety of reasons, and it is definitely simpler to do mathematics with the Axiom of Choice rather than without it. ***The preceding applications to transfinite cardinal numbers strongly illustrate this point.***

This leads directly to the issue of ***whether the Axiom of Choice should be included in our axioms for set theory.*** As indicated above and in these notes, the assumption of the Axiom of Choice allows mathematicians to do many things that would otherwise be difficult or impossible. Although some mathematicians think that the subject should only consider objects given by suitably "constructive" methods, the existence and other consequences the Axiom of Choice are so useful and powerful that most mathematicians would prefer to include it as part of the axioms if at all possible. By the middle of the 20th century the Axiom of Choice was generally accepted (but in many cases grudgingly) by most "ordinary" mathematicians — ***i.e.***, most of those who are not logicians or set theorists.

Here are some further online references for the Banach – Tarski paradox.

http://mathworld.wolfram.com/Banach-TarskiParadox.html

http://www.math.hmc.edu/~su/papers.dir/banachtarski.pdf

http://www.kuro5hin.org/story/2003/5/23/134430/275

http://en.wikipedia.org/wiki/Banach-Tarski_Paradox

Relative consistency of the Axiom of Choice

Of course, if the Axiom of Choice leads to a logical contradiction, then it should not be part of the axioms for set theory, so this brings us back to the first question. Two extremely important and fundamental pieces of research by K. Gödel in the nineteen thirties clarified the role of the Axiom of Choice. The first of these was his work on the incompleteness properties of axiomatic systems, and the essential conclusion is that mathematics can ***never*** be absolutely sure that ***any*** reasonable set of axioms for an infinite set theory is logically consistent. His subsequent result showed that the Axiom of Choice was ***relatively consistent*** with the other axioms for set theory. Specifically, ***if there is a logical contradiction in set theory with the inclusion of the Axiom of***

Choice, then there is also a logical contradiction if one does not assume the Axiom of Choice. This is entirely analogous to the situation for the Axiom of Foundation that was discussed in Section **III.4** of these notes.

Formally, the relatively consistency properties are often stated in terms of the system of axioms for set theory developed by E. Zermelo (1871 – 1953) and A. Fraenkel (1891 – 1965) which is generally known as **ZF**. In these terms, Gödel's results state that if **ZF** plus either the Axiom of Foundation or the Axiom of Choice is logically inconsistent, then **ZF** is already logically inconsistent **without** either assumption.

Here are some further online references related to these topics:

http://planetmath.org/encyclopedia/MultiplicativeAxiom.html

http://mathworld.wolfram.com/AxiomofChoice.html

http://www.miskatonic.org/godel.html

http://www.time.com/time/time100/scientist/profile/godel.html

http://en.wikipedia.org/wiki/Kurt_Gödel

http://scienceworld.wolfram.com/biography/Goedel.html

http://www.cs.uwaterloo.ca/~alopez-o/math-faq/node69.html

Since most mathematicians would prefer to include as many objects as possible in set theory so long as these objects do not lead to a logical contradiction, the effective consequence of relative consistency is that inclusion of the Axiom of Choice in the axioms for set theory is viewed as appropriate by most "ordinary" mathematicians. From a purely formal viewpoint, there is nothing to lose and much to gain by adding this extra assumption. The system obtained by including the Axioms of Foundations and Choice with **ZF** is frequently denoted by **ZFC**.

Axiomatic systems for set theory. Having mentioned **ZF**, we should note that our approach to set theory is slightly different because our setting includes collections called classes that are too large to be sets while **ZF** does not (in **ZF** such objects simply do not exist). Our formulation is based on a variant of **ZF** that is due to von Neumann, P. Bernays (1888 – 1977) and Gödel, and is often denoted by **NBG**; this formulation is closely related to **ZF** and is very widely used (although this is generally not stated explicitly outside of mathematical writings on set theory and the foundations of mathematics). As suggested by the first sentence in this paragraph, one major innovation in the latter is its use of classes for collections that are too large to be sets. Another important difference is that the Axiom of Specification is simplified very substantially (in particular, it is replaced by a finite list of assumptions). Both formulations yield the same logical consequences, and each is logically consistent if and only if the other is. This equiconsistency of **ZF** and **NBG** was established in the 1960s and is generally attributed to W. Easton (1939 –) and R. Solovay (1938 –). The following online references contain additional information about both **ZF** and **NBG**:

http://en.wikipedia.org/wiki/ZFC

http://www.bookrags.com/Zermelo%E2%80%93Fraenkel_set_theory

http://mathworld.wolfram.com/vonNeumann-Bernays-GoedelSetTheory.html

http://en.wikipedia.org/wiki/Von_Neumann-Bernays-G%C3%B6del_axioms

Having noted the impossibility of proving that set theory is logically consistent, the next question is more or less unavoidable.

What if set theory is logically inconsistent? Although we can never be absolutely sure about this, there is a great deal of encouraging evidence. The basic axiomatic structure for set theory has now been in place and in its current form for about three quarters of a century, and no new concerns have arisen over that time. Of course, there are no guarantees that new difficulties will never emerge, but the absence of new problems over 75 years of intense critical study of foundational questions and enormous progress in all areas of mathematics lead to an important subjective conclusion: ***The current axiomatic system has proven to be highly reliable even if we cannot be sure it is absolutely perfect.***

Even if some new problems arise, most mathematicians strongly believe that they can be handled effectively, and the following annotated quote from the first page of the online document

http://www.math.ku.dk/~kiming/courses/2004/matm/real_numbers.pdf

seems worth including at this point:

> Do not worry too much about this [*the possibility that there are some hidden contradictions*] **...** No contradictions have turned up after a century of scrutiny, and if a contradiction should turn up you can be sure that bridges will not suddenly start to collapse [*because of such a contradiction*] or that space ships will miss their destinations because of that [*of course, this might happen for other reasons*]. If a contradiction turned up we would simply have to reconsider the situation and construct a new axiomatic system that does for us what we want of it [*this would probably be far more difficult than the comments suggest, but in principle it would resemble the sort of work that is needed whenever one finds a nontrivial logical problem in some complicated piece of computer software that has proven to be pretty reliable over an extended period of time — everyone is confident that the program can be repaired, but a great deal of time and effort may be needed to complete the job*].

Logical independence of the Axiom of Choice

Fundamental results of P. M. Cohen (1934 – 2007) from the 1960s have completed our current understanding of the logical status of the Axiom of Choice. Specifically, he showed that one can construct models for set theory such that the Axiom of Choice was true for some models and false for others; this conclusion is slightly more concrete than the one obtained by Gödel, which did not yield comparable information about constructing alternative models for set theory. Here are some online references with further information:

http://plato.stanford.edu/entries/set-theory/#7

http://publish.uwo.ca/~jbell/CHOICE.pdf

http://en.wikipedia.org/wiki/Axiom_of_choice#Independence

http://www-math.mit.edu/~tchow/mathstuff/forcingdum

http://en.wikipedia.org/wiki/Forcing_(mathematics)

There are also several weaker statements which are not equivalent to the axiom of choice**,** but which are closely related**.** One simple one is the ***Axiom of Countable Choice*****,** which states that a choice function exists for any ***countable*** set **X.** It states that a ***countable*** collection of sets must have a choice function**.** The previously mentioned methods and results of P. Cohen also show that the Axiom of Countable Choice is not provable in **ZF.**

The Axiom of Countable Choice is required for the rigorous development of calculus and the theory of functions of a real variable in its standard form**;** in particular**,** many results in these subjects depend on having a choice function for a countable set of real numbers (considered as sets of Cauchy sequences of rational numbers)**.** Some mathematicians who have reservations about the Axiom of Choice are willing to accept the Axiom of Countable Choice**.**

VII. 6 : The Continuum Hypothesis

(Halmos, § 25)

The third issue raised above was whether there are other statements which might deserve to be taken as axioms for set theory**.** One widely known statement of this type is the the ***Continuum Hypothesis*****,** which emerged very early in the study of set theory**.**

CONTINUUM HYPOTHESIS. *If* **A** *is an infinite subset of the real numbers* $\mathbb{R}$**,** *then either there is a* $\mathbf{1-1}$ *correspondence between* **A** *and the natural numbers* $\mathbb{N}$**,** *or else there is a* $\mathbf{1-1}$ *correspondence between* **A** *and* $\mathbb{R}$**.**

This question arose naturally in Cantor's work establishing set theory**,** the motivation being that he did not find any examples of subsets whose cardinal numbers were strictly between those of $\mathbb{N}$ and $\mathbb{R}$**.**

Since there is a $\mathbf{1-1}$ correspondence between the real numbers $\mathbb{R}$ and the set $\mathbf{P(\mathbb{N})}$ of all subsets of $\mathbb{N}$**,** one can reformulate this as the first case of a more sweeping conjecture known as the **Generalized Continuum Hypothesis:**

GENERALIZED CONTINUUM HYPOTHESIS (GCH). *If* **S** *is an infinite set and* **T** *is a subset of* **P(S),** *then* **either**

(1) *there is a one-to-one correspondence between* **T** *and a subset of* **S, *or else***

(2) *there is a one-to-one correspondence between* **T** *and* **P(S).**

In analogy with his results on the Axiom of Choice**,** the work of Gödel showed that if a contradiction to the axioms for set theory arose if one assumes the Continuum Hypothesis or the Generalized Continuum Hypothesis**,** then one can also obtain a

contradiction without such an extra assumption. On the other hand, the previously mentioned fundamental work of P. M. Cohen shows that one can construct models for set theory such that the Continuum Hypothesis was true for some models and false for others. In fact, one can construct models for which the number of cardinalities between those of $\mathbb{N}$ and $\mathbb{R}$ can vary to some extent; some aspects of this are discussed below.

Because of Cohen's results, many mathematicians are ***not*** willing to assume the Continuum Hypothesis or the Generalized Continuum Hypothesis for the same reason that they are willing to assume the Axiom of Choice: They would prefer to include as many objects as possible in set theory so long as these objects do not lead to a logical contradiction. Cohen's own viewpoint on this matter is summarized in the third online reference listed below.

Here are some online references which discuss Cohen's methods and results:

http://mathworld.wolfram.com/ContinuumHypothesis.html

http://en.wikipedia.org/wiki/Forcing_(mathematics)

http://en.wikipedia.org/wiki/Paul_Cohen_(mathematician)

Cohen's methods show that several other natural questions in set theory are true in some models but false in others; the preceding references contain details on numerous results of this type. We shall limit our discussion to a related question concerning cardinal numbers:

> *Suppose that* **A** *and* **B** *are sets whose power sets satisfy the cardinality equation* $|\mathbf{P(A)}| = |\mathbf{P(B)}|$. *Does it follow that* $|\mathbf{A}| = |\mathbf{B}|$**?**

For finite sets this is a trivial consequence of the fact that the function $\mathbf{2^x}$ is strictly increasing over the real numbers. For infinite sets, there is a curious relation between this question and the Generalized Continuum Hypothesis: *If the latter is true, then the answer to the question is* **YES.** This follows because for every infinite set **A** we know that $|\mathbf{P(A)}|$ is the unique first transfinite cardinal number that is strictly larger than $|\mathbf{A}|$, and conversely $|\mathbf{A}|$ is the largest cardinal number that is strictly less than $|\mathbf{P(A)}|$.

On the other hand, the condition on cardinal numbers is not strong enough to imply the Generalized Continuum Hypothesis, and one can also construct models of set theory containing sets **A** and **B** such that $|\mathbf{A}| < |\mathbf{B}|$ but $\mathbf{2}^{|\mathbf{A}|} = \mathbf{2}^{|\mathbf{B}|}$. More generally, very strong results on the possible sequences of cardinal numbers that can be written as $\mathbf{2}^{|\mathbf{A}|}$ for some $|\mathbf{A}|$ are given by results of W. B. Easton which build upon Cohen's methods; Easton's result essentially states that a few relatively straightforward necessary conditions on such sequences of cardinal numbers are also sufficient to realize it as the set of cardinalities for power sets. These results first appeared in the following paper by Easton: ***Powers of regular cardinals***, Ann. Math Logic **1** (1970), 139 – 178. A more recent paper by T. Jech (pronounced ye~~KH~~, with ~~KH~~ as in the "ch" of "Bach") covers subsequent work on this problem: ***Singular cardinals and the* PCF *theory***, Bull. Symbolic Logic **1** (1995), 408 – 424.

Possibilities for the cardinality of the real numbers. Since Cohen's results imply that $|\mathbb{R}|$ may or may not be equal to $\aleph_1$ depending upon which model for set theory is being considered, one can ask which cardinal numbers are possible values for $|\mathbb{R}|$. Results on this and more general questions of the same type follow from Easton's work. In particular, it turns out that $|\mathbb{R}|$ can be equal to $\aleph_n$ for every positive integer **n** but it

cannot be equal to the cardinal number $\aleph_\omega$ (all these are defined as above). A proof of the last assertion appears in the exercises on page 66 of the following book:

> I. Kaplansky, ***Set theory and metric spaces*** (2nd Ed.). Chelsea, New York, 1977. ISBN: 0–8284–0298–1.

Recently there has been some further thought about whether or not one should assume the Continuum Hypothesis, and much of it has been generated by the following articles:

> W. H. Woodin, *The continuum hypothesis*, Parts **I – II**. Notices of the American Mathematical Society **48** (2001), 567 – 576, 681 – 690. [Available online at **http://www.ams.org/notices/200106/fea-woodin.pdf** and **http://www.ams.org/notices/200107/fea-woodin.pdf**.]

The following online site includes a fairly extensive scholarly analysis of Woodin's articles:

http://www.math.helsinki.fi/logic/LC2003/presentations/foreman.pdf

VIII : Set theory as a foundation for mathematics

This material is basically supplementary, and it was not covered in the course. In the first section we discuss the basic axioms of set theory and the desirability of making the axiom system as simple and irredundant as possible. The main objective of the second section is to describe exactly how one can simplify our assumptions for set theory, with particular attention to our fairly lengthy set of axioms for number systems. It turns out that one can replace these by a single assumption that is far more concise and is also central to the basic logical consistency issues raised in the previous unit. In the third section we prove results stated in Unit **V** about the essential uniqueness of number systems satisfying our axioms for the integers and the real number system. The fourth and final section covers a topic that fits in with both the naïve and formal approaches. In Unit **I** of these notes we mentioned that the axioms for Euclidean geometry were viewed as a major portion of the logical foundations for mathematics up to the early 19th century, and that by the end of that century set theory was quickly evolving into a new logical basis for the subject. One natural question is whether the axioms for classical Euclidean geometry can be integrated into the new framework for mathematics, and if so the next question is how this can be done. In the final section we explain how one can view the classical axiomatic approach to geometry within the environment of set theory.

VIII. 1 : Formal development of set theory

(Halmos, §§ 1 – 10, 14; Lipschutz, § 1.12)

In Section **II.1** we began by describing set theory from a naïve viewpoint and then indicated how one could set things up more formally. In most of the notes, our approach has been very much on the naïve side; usually we have introduced assumptions about set theory as they were needed to continue or expedite the discussion without worrying too much about how one should express everything in a completely rigorous manner. This allowed us to develop the subject fairly rapidly. At some points we mentioned the need to be more specific about some issues (***e.g.***, describing the "admissible" logical statements that can be used to describe sets) or the possibility of deriving some of our assumptions as logical consequences of the others. For example, in Section **III.2** of the notes we mentioned that the existence of objects with the properties of ordered pairs can be proved from the other assumptions; details appear on pages 23 – 25 of Halmos. Frequently the proofs of such implications are somewhat complicated and unmotivated and the approach may seem artificial, and therefore we have simply added assumptions in Section **III.2** and elsewhere to save time and to focus attention on points that are directly related to the uses of set theory in the mathematical sciences.

However, once the basics of set theory have been covered and assimilated, there are some extremely compelling reasons to look back and examine the assumptions in order to see if they can be simplified and redundant assumptions can be eliminated.

One major reason to look for simpler and more concise assumptions is a basic principle in the philosophy of science called ***Ockham's razor***, which was originally stated by William of Ockham (1285 – 1349). In modern language, this principle states that

complications should not be introduced unless they are necessary

or in more imperative terms

do not invent unnecessary entities to explain something.

Since we shall appeal to Ockham's razor at other points in this unit, we include an online reference to a biography for William of Ockham:

http://plato.stanford.edu/entries/ockham/

In the mathematical sciences there are important practical justifications for using Ockham's razor that go well beyond simplicity of exposition. Since the mathematical sciences are so heavily dependent upon deductive logic, it is absolutely essential to have some assurance that the basic assumptions are logically sound. If the assumptions for some theory lead to logical contradictions, serious questions arise about the validity and reliability of the theory's conclusions and value. ***Simplified lists of basic assumptions turn out to be extremely useful for testing the logical soundness of a mathematical system.*** The reason is obvious; there are fewer things to verify, for much of the work is redirected into verifying the original assumptions are equivalent to the simplified ones.

The advantages of simplified lists of assumptions are also illustrated very clearly by examples within mathematics itself. In mathematical proofs by contradiction, the underlying idea for proving **P** implies **Q** is to assume that **P** is true, to add an assumption that **Q** is false, and to use the new, longer set of hypotheses to obtain a contradiction. This method has a fundamental implication: ***As lists of assumptions become longer and more complicated, one must be increasingly careful in checking whether the entire list of assumptions is logically consistent.*** It is generally much easier to check shorter systems of axioms for consistency than it is to check longer ones, so if we want to understand the consistency properties of our axioms it is highly desirable to have an equivalent version which is as simple as possible.

Summary of the basic axioms

As noted in Unit **VII**, one standard axiomatic approach to set theory in present day mathematics is based upon axioms introduced by E. Zermelo during the first decade of the 20th century, with a few subsequent modifications due to other mathematicians, most notably A. Fraenkel. Versions of most ***Zermelo – Fraenkel*** (**ZF**) ***axioms*** have been introduced in previous units, and all the other assumptions we have introduced turn out to be consequences of these axioms, all of which are listed below:

- The Axiom of Extensionality (see Section **II.1**)
- The Axiom of Pairs (see Section **II.2** and also below)
- The Axiom of Specification (see Section **II.2**)
- The Axiom of the Power Set (see Section **III.3**)

- The Axiom of Unions (see Section **III.3**)
- The Axiom of Replacement (see Section **IV.4**)
- The Axiom of Foundation (see Section **III.5**)
- The Axiom of Number Systems (see Sections **V.1** and **V.4** as well as the next paragraph)

Note that the Axiom of Choice is missing from this list; if this is added, one obtains the system called **ZFC** in the previous unit. Since a few of the **ZF** axioms have not yet been formulated explicitly, we shall explain the latter in more detail. Given two objects **a** and **b**, the ***Axiom of Pairs*** formally states the existence of the set we have called **{a, b}**. A close inspection of the underlying logical principles reveals a need to make such an assumption in addition to the Axioms of Specification and Unions; in particular, something like this is needed to ensure that sets actually exist in our abstract logical system. The ***Axiom of Number Systems*** is actually not in the usual version of **ZF,** but it represents our assumption that the integers and real number systems are sets; much of this unit will be devoted to discussing the drastically simplified version of this axiom which is part of the usual **ZF** axioms.

As noted in Section **VII.5,** our formulation of set theory in these notes is based on a variant of **ZF** that is due to von J. Neumann, P. Bernays and K. Gödel and called **NBG;** this formulation is closely related to **ZF** and is perhaps the most widely used (although this is generally not stated explicitly outside of mathematical writings on set theory and the foundations of mathematics). One major feature in the latter is its use of **classes** for collections that are too large to be sets; in **ZF** these are not regarded as legitimate objects of any sort. Another important difference is that the Axiom of Specification is simplified in a significant manner. As noted earlier, both formulations yield the same logical consequences, and one is logically consistent if and only if the other is.

We have already given a few online references for the usual axioms of set theory. Here is one more:

http://mathworld.wolfram.com/Zermelo-FraenkelAxioms.html

VIII. 2 : Simplified axioms for the basic number systems

(Halmos, §§ 11 – 13)

Units **II** through **VII** covered the basic material in set theory that is needed to use the latter in the mathematical sciences, and this section discusses two basic issues. One, which has already been discussed at some length, concerns the logical consistency problems that follow from Gödel's Incompleteness Theorem. The other is to replace our fairly lengthy set of axioms for the real number system by something that is more concise but logically equivalent. We have already noted the important relationship between these two issues in the preceding section.

As we have already stated, the logical incompleteness results of Gödel imply that we can never be completely sure that any "reasonable" system of axioms for set theory like **ZF** (Zermelo – Fraenkel) is logically consistent. However, by the relative consistency results of Gödel that we have also discussed, neither the Axiom of Choice nor the (Generalized) Continuum Hypothesis is a potential source of consistency problems. In view of all these results, it is natural to ask where such potential difficulties might lie. There are many similarities between the Axiom of Choice and the Axiom of Foundation; both seem reasonable and both make it easier to discuss some mathematical topics, but both are basically *nonconstructive existence statements*. One further similarity is that there are Gödel relative consistency results for both the Axioms of Foundation and Choice: *If the standard* **ZFC** *axioms for set theory are logically inconsistent, then the system* **ZF** *without the Axiom of Choice is also logically inconsistent. Furthermore, if* **ZF** *is logically inconsistent, then* **ZF** *without the Axiom of Foundation is also logically inconsistent.*

Among the remaining axioms, the next natural candidates are those dealing with something that is infinite. There are two axioms of this type in **ZF**, one of which is the *Axiom of Infinity* — which assumes the existence of an infinite set — and the *Axiom of Specification* — which is really an ***infinite*** (in fact, countably infinite) ***list of axioms***, one for each of the admissible statements that can be used to define a set. In our setting, one can prove rigorously that if there is an internal contradiction in the **ZF** axioms for set theory, it must arise either from

(1) the assumptions about constructing sets with definitions given by fairly general types of valid mathematical statements, or from

(2) the assumptions about the existence of the real numbers and its standard hierarchy of subsystems including the natural numbers (nonnegative integers), the (signed) integers and the rational numbers.

Problems concerning the first point arose at the end of the 19th century and the beginning of the 20th century, and two of these are the previously mentioned paradoxes of B. Russell and C. Burali – Forti. We have already noted that mathematicians and logicians resolved these problems by suitably restricting the class of admissible grammatical statements for specifying sets and by adding an axiom which guarantees, among other things, that a set cannot be a member of itself. All of this has now been in place and in its current form for over three quarters of a century. During the intervening time, no additional problems involving the first point have arisen; of course, there are no guarantees that new difficulties will never emerge. However, the absence of new problems over 80 years of intense critical study of foundational questions and enormous progress in all areas of the mathematical sciences lead to an important subjective conclusion: The current Axiom of Specification is highly reliable even if we cannot be sure it is absolutely perfect. Confidence in this respect is reinforced by the **NBG** formulation of set theory due to von Neumann, Bernays and Gödel that we discussed in Section **VII.5.** The crucial feature of **NBG** is that ***the latter reduces the Axiom of Specification to a* FINITE *list of assumptions at the expense of assuming the existence of "proper classes" that are not sets.***

As noted in Section **VII.5,** even if some new problems eventually arise, most if not all mathematicians strongly believe that they can be handled effectively, although this could very well take a considerable amount of time and effort. It does not seem likely that such repairs would have much effect on most of the mathematics that is currently known, and it is even less likely that there would be any real effect on the applications of the subject (but there might be exceptions for subjects like modern theoretical physics which rely particularly heavily on mathematical ideas). However, we can never be absolutely certain of this.

We now turn to the second point regarding our axioms for number systems. ***Given the numerous assumptions we have made about the real number system, one* MUST NOT *simply ignore the possibility that they could be manipulated to derive a logical contradiction.*** Of course, many of the assumptions about algebraic equations and inequalities are quite standard, and many are just refinements of the simple assumptions (the "common notions") at the beginning of Euclid's ***Elements***. However, there are two aspects of the axioms for the real numbers that are especially problematic:

A. The existence of infinite sets (for example, the real numbers) is assumed.

B. There is a strong assumption about the existence of least upper bounds that is far less elementary than the other assumptions on equations and inequalities and goes beyond the standard properties of arithmetic operations and inequalities. Formally, **this is another example of a nonconstructive existence statement.**

The standard axioms for set theory

Since the existence of infinite number systems is absolutely central to mathematics, it should be clear that we cannot avoid making some assumption about the existence of an infinite set. A major goal of this section is to indicate how one can use such an axiom to prove the existence of a system which satisfies all the properties we assumed for the real number system. Once this is done, we can use the principle of Ockham's razor to simplify out axioms for set theory to the following:

1. The axioms listed in the preceding section, ***except*** for the Axiom of Number Systems, which is related to the Standard Axiom of Infinity.

2. A simply stated ***Standard Axiom of Infinity***, which is given below.

3. The ***Axiom of Choice*** or an equivalent statement (***e.g.***, the Well – Ordering Property or Zorn's Lemma).

Here is the formal statement of the axiom mentioned in the second point on the list:

STANDARD AXIOM OF INFINITY. *There is a set* ω *such that the following hold*:

(1) *The empty set* $\varnothing$ *belongs to* ω.

(2) *For each* $x \in \omega$, *we also have* $x \cup \{x\} \in \omega$.

(3) *If* **A** *is an arbitrary subset of* ω *satisfying the preceding two conditions when* ω *is replaced by* **A**, *then* $A = \omega$.

This axiom corresponds to a model for the nonnegative integers in which $\emptyset$ corresponds to **0** and $x \cup \{x\}$ corresponds to $x + 1$, and the axiom merely says that ***this specific infinite class is a set.***

We can check directly that this set ω satisfies Peano Axioms, with $\sigma(x) = x \cup \{x\}$, as follows: If $y = \sigma(x)$ for some x, then $x \in y$ and hence y is nonempty. Therefore the empty set cannot be equal to $\sigma(x)$ for any x. Next, we need to show that σ is $1 - 1$. Suppose however that $\sigma(x) = \sigma(y)$. Then we have $x \cup \{x\} = y \cup \{y\}$. If x and y are unequal this can only happen if $x \in y$ and $y \in x$; but the Axiom of Foundation implies that these cannot both be true, which means that $x = y$, so that σ is $1 - 1$. Finally, if M is a subset of ω which contains $\emptyset$ and such that $x \in M$ implies $\sigma(x) \in M$, then the third condition in the Standard Axiom of Infinity implies $M = \omega$. ■

In claiming that the simplified axiom list given above is adequate to yield everything we have done in these notes, we are asserting in particular that

the existence of an object with all the properties of the real number system exists under these assumptions.

The remainder of this section will explain why this is true. The basic idea is to ***construct a system satisfying all the properties of the real numbers*** using the simplified axiom list in which the assumption on ω replaces the Axiom of Number Systems. We shall not attempt to include all the details; most turn out to be fairly routine arguments, but the work is often tedious. Instead, our main emphasis will be to explain the ideas in the construction. Here are some online references which cover the details in an extremely thorough manner.

http://www.math.nus.edu.sg/~urops/Projects/RealNumbers.pdf

http://www.math.ku.dk/~kiming/courses/2004/matm/real_numbers.pdf

The first reference covers everything, and the second concentrates on Cantor's construction of the real numbers which is described below.

Showing the existence of a object with all the properties of the real number system requires the following preliminary steps:

1. It is necessary to construct the arithmetic operations and linear ordering on the standard model for the Peano axioms.
2. It is necessary to construction of the (signed) integers from the standard model for the Peano axioms.
3. It is necessary to construct the rational numbers from the integers.
4. It is necessary to construct the real numbers from the rationals.

We shall consider each of these in the order listed.

Arithmetic operations, linear ordering and the Peano axioms

Before we can think of constructing the integers or anything else that is larger than the natural numbers $\mathbb{N}$, we need to define addition and multiplication on an abstract system satisfying the Peano axioms and verify that they have the usual properties. The

following recursive definitions of addition, multiplication, and exponentiation are standard, and in particular they appear on page 51 of Goldrei.

(1) **ADDITION** $n + k$: $n + 0 = n$ *and* $n + \sigma(k) = \sigma(n + k)$.

(2) **MULTIPLICATION** $n \times k = n \cdot k$: $n \cdot 0 = 0$ *and* $n \cdot \sigma(k) = (n \cdot k) + n$.

(3) **EXPONENTIATION** $n^k = n\text{^}k$ (*provided* $n \neq 0$) : $n\text{^}0 = 1$ *and* $n\text{^}\sigma(k) = (n\text{^}k) \cdot n$. (*If* $n = 0$, *then we define* $0\text{^}k = 0$ *for all* $k \neq 0$).

The familiar basic arithmetic rules for these operations are stated in Theorem 3.12 on page 53 of Goldrei. These include the commutative and associative laws of addition and multiplication, the distributive law, and the three standard laws of (integral) exponents:

$(m \cdot n)\text{^}k = (m\text{^}k) \cdot (n\text{^}k)$, $(n\text{^}a)\text{^}b = n\text{^}(a \cdot b)$, $(n\text{^}a) \cdot (n\text{^}b) = n\text{^}(a + b)$

Further arithmetic rules appear on pages 53 – 56; most of these are identities for special cases when n or k is equal to 0 or 1.

The definition of inequality is very easy in this standard model for the Peano axioms; namely, $n < m$ if and only if $n \in m$. The basic properties of inequalities (*e.g.,* for unequals added to or multiplied by equals) are stated in Theorem 3.13 on page 56, with some further properties listed on the next page.

Construction of the (signed) integers and rational numbers

If one thinks as the (signed) integers as an extension of the natural numbers to allow arbitrary subtraction and the rational numbers as an extension of the integers to allow division by a nonzero integer, it is not surprising that the construction of the integers from the natural numbers and the construction of the rational numbers from the integers should be similar.

Construction of the integers. It is useful to begin by stating exactly what we need to do. Using the existence of a Peano system we are supposed to construct a set $\mathbb{Z}$ together with binary operations $A: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ and $M: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ that correspond to addition and multiplication respectively, we are also supposed to construct a linear ordering on $\mathbb{Z}$, and finally we are supposed to show that these three operations satisfy the properties that were listed in Section V.2.

We have already stated that we want the integers to be a system in which subtraction is always possible, and the key idea in the construction is to start with ordered pairs of natural numbers that we shall think of as formal difference expressions. Of course, two difference expressions $a - b$ and $c - d$ may yield the same number, so we need to identify two difference expressions that yield the same value. It is a very easy exercise in algebra to see that $a - b = c - d$ is true if and only if $a + d = b + c$; the second equation is meaningful within the natural numbers, so we can state our condition for formal differences to be the same using a binary relation given by a subset of $\mathbb{N} \times \mathbb{N}$:

Definition. Two elements (a, b) and (c, d) of $\mathbb{N} \times \mathbb{N}$ are ***formal difference equivalent*** if $a + d = b + c$.

The name of the relation suggests that formal difference equivalence should be an equivalence relation, and in fact this is true. The proof is a fairly straightforward exercise. As on page 32 of Goldrei, we may now ***define*** the integers $\mathbb{Z}$ to be ***the set of all equivalence classes of this equivalence relation.*** There is a natural embedding of $\mathbb{N}$ into $\mathbb{Z}$ given by sending **n** to the equivalence class of **(n, 0)**.

The next step is to define addition, multiplication and ordering on $\mathbb{Z}$ so that it extends the given definitions on $\mathbb{N}$. It is easy to guess what sorts of properties the correct definitions should have.

Provisional definitions. Suppose we are given integers **x** and **y** with representatives **(a, b)** and **(c, d)** respectively. Then the sum **x + y** should be represented by the ordered pair **(a + c, b + d)**, the product **x · y** should be represented by the more complicated ordered pair **(ac + bd, bc + ad)**, and the strict linear ordering **x < y** should be equivalent to **a + d < b + c**.

One fundamental issue with this provisional definition is that the ***output is given by choosing representatives for the equivalence classes*** **x** and **y**. Since we want functions that are single valued, we need to show that any other choices of representatives for the equivalence classes will yield the same element of $\mathbb{Z}$. In standard mathematical terms, ***we must show that our constructions of addition, multiplication and ordering are*** **well – defined**. This required verifying the three items in the following statement.

Well – definition of operations. *In the notation above, suppose that* **(p, q)** *and* **(a, b)** *represent the same element of* $\mathbb{Z}$, *and likewise that* **(r, s)** *and* **(c, d)** *represent the same element of* $\mathbb{Z}$. *Then each of the following pairs also represent the same element of* $\mathbb{Z}$**:**

- *The pairs* **(a + c, b + d)** *and* **(p + r, q + s)**.
- *The pairs* **(ac + bd, bc + ad)** *and* **(pr + qs, qr + ps)**.
- *The inequality* **a + d < b + c** *is true if and only if* **p + s < q + r** *is true.*

Verifying the preceding statements requires a series of elementary but fairly tedious calculations; these are all carried out in the first online document cited above.

The preceding defines addition, multiplication and ordering for the integers, and the next steps are to show that the definitions extend the ones for $\mathbb{N}$ and have all the required properties listed in Section **V.1**. Once again, the details may be found in the first online document in our list. The verifications are elementary but somewhat tedious; the standard advice is that "every mathematician should go through the details once and understand them, but not worry about committing them to memory."

Construction of the rational numbers. We are now ready to discuss the construction of the rational numbers from the integers. This is done on pages 29 – 31 of Goldrei with some motivation on page 28.

As we have already noted, the construction of the rational numbers from the integers is supposed to allow division by nonzero quantities, and following the previous construction we begin by considering ordered pairs of integers (with the second one nonzero) to be formal quotients. This is slightly different from the approach in Goldrei,

where the denominator is assumed to be positive, but one ultimately obtains the same system regardless of whether the denominators are assumed to be positive or merely to be nonzero.

One standard condition for two ratios of integers **a/b** and **c/d** to be equal is **ad = bc.** One may use this to define rational numbers using ordered pairs of integers **(x, y)** such that the second term is nonzero, and saying that two elements **(a, b)** and **(c, d)** of the set $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ are ***formal quotient equivalent*** if **a·d = b·c.**

The name of the relation suggests that formal quotient equivalence should be an equivalence relation, and in fact this is true. The proof is a fairly straightforward exercise. As on page 29 of Goldrei, we may now ***define*** the rational numbers $\mathbb{Q}$ to be ***the set of all equivalence classes of this equivalence relation.*** There is a natural embedding of $\mathbb{Z}$ into $\mathbb{Q}$ given by sending the integer **a** to the equivalence class of **(a, 1).**

We can now formulate provisional definitions for addition, multiplication and ordering. The underlying idea is the same as for the construction of the integers, but the formulas will be much different. Suppose we are given rational numbers **x** and **y** with representatives **(a, b)** and **(c, d)** respectively. Then the sum **x + y** should be represented by the ordered pair **(ad + bc, bd),** the product **x·y** should be represented by the more complicated ordered pair **(ac, bd),** and the strict linear ordering **x < y** should be equivalent to $abd^2 < b^2cd$. — Since the latter differs from Goldrei and is clearly more complicated than anything else in sight, we should explain it. A ratio **u/v** will be positive if and only if the product of the numerator and the denominator is positive, and **a/b < c/d** should hold if and only if the difference **(c/d) – (a/b)** is positive. The latter fraction is equivalent to **(bc – ad)/bd,** and the product of this fraction's numerator and denominator is simply $b^2cd - abd^2$.

In analogy with the construction of integers, the next step is to verify that these constructions do not depend upon the choices of representatives for **x** and **y.** This is covered fairly explicitly on pages 29 – 30 of Goldrei, and because of this and the similarity to the integral case we shall not state all the details here. These are also verified in the first online document cited above, and the advice at the end of the discussion of the integers applies here equally well. One additional point to be checked is that the new definitions of addition, multiplication and ordering coincide with the previous ones on the integers; ***i.e.,*** those formal quotients whose denominators are equal to **1.** This is a tedious but extremely simple exercise, and the argument contains no surprises.

To complete the discussion of the rational numbers, we need to show that they have the standard fundamental properties along the lines of Unit **V.** Specifically, these include all the properties of the real numbers except the Dedekind Completeness Property.

The Dedekind construction of the real numbers

At certain points when it was necessary for ancient Greek mathematicians to compare irrational numbers, this was done using an idea essentially due to Eudoxus of Cnidus (408 – 355 B.C.E.), which we state in modern language:

Condition of Eudoxus. *Two real numbers* **x** *and* **y** *are equal if and only if the following two statements hold*:

(1) *Every rational number less than* **x** *is also less than* **y**.
(2) *Every rational number greater than* **x** *is also greater than* **y**.

One proves this result as follows: If **x** and **y** are unequal, say **x < y**, then there is a rational number **b** between them, and this rational number **b** is greater than **x** but less than **y**. Similar considerations apply if **x > y**. ■

In particular, the Condition of Eudoxus plays an important role in the theory of irrational geometric proportions as developed in Euclid's ***Elements***.

During the late 1850s, R. Dedekind took these ideas one important step further. For each real number **a**, the set of all rational numbers that are less than **a** has some easily stated properties, and Dedekind's idea was that a converse was true; namely, a set of rational numbers which looks like it could be a set defined by a number actually arises from a real number. The treatment on pages 8 – 17 of Goldrei is slightly different from Dedekind's in some respects, but it is closely related and yields an equivalent object. For the sake of completeness, here is a reference to a readily available book which contains Dedekind's fundamental (and still very readable) paper, ***Continuity and irrational numbers.***

> R. Dedekind, ***Essays on the Theory of Numbers*** (Authorized Translation by W. Beman). Dover, New York, 1963. ISBN: 0–486–21010–3.

Later in this unit we shall indicate how ***Dedekind's approach to the real numbers depends very substantially on being able to work effectively with infinite sets.***

In order to proceed, we need to formalize the notion of "a set of rational numbers which looks like it could be a set defined by a number" in the preceding paragraph. The following definition appears on page 9 of Goldrei.

Definition. A nonempty set **S** of rational numbers is a ***left Dedekind set*** (or the ***left half of a Dedekind cut***) if it has the following properties:

1. The set **S** has an upper bound.

2. The set **S** has no largest element.

3. If **x < y** and **y ∈ S**, then **x ∈ S**.

Strictly speaking, a left Dedekind cut consists of **two** sets, one of which is given above and the other, the right half, is the relative complement. Every rational number **q** determines a left Dedekind set, which is merely the set of all rational numbers that are less than **q**. Verifying the three conditions for such a set is a straightforward exercise.

In Dedekind's approach, one **defines** the real numbers to be the collection of all left Dedekind sets; the axioms of set theory will then imply that this collection is a set.

The next step is to define addition, multiplication and ordering for left Dedekind sets. It is particularly easy to define ordering, for it corresponds to set – theoretic inclusion. With this definition, the important Dedekind Completeness Property follows very quickly; in fact, the ***least upper bound*** of a bounded collection of left Dedekind sets turns out to be the ***union*** of these sets (see Goldrei, Theorem 2.2, pages 13 – 14).

Defining addition is a little less trivial but still not difficult. Given two left Dedekind sets **C** and **D**, the *sum* **C + D** is taken to be the set of all rational numbers expressible as **x + y** where **x ∈ C** and **y ∈ D.** One needs to check that this is again a left Dedekind set**,** but this can be done**.** It is also useful to describe the negative of a left Dedekind set **C** at this point**.** Let $\mathbf{B_0}$ denote the complement of **C** in the rational numbers**,** and take **B** equal to $\mathbf{B_0}$ if the latter has no least element **m** and $\mathbf{B = B_0 - \{m\}}$ otherwise**;** finally define the ***negative*** **– C** to be the set of all numbers **x** such that **– x ∈ B.**

CLAIM: *The set* **– C** *is a left Dedekind set.*

Proof. The first thing to note is that this set is nonempty**,** or equivalently that **B** is nonempty**.** The first two conditions on **C** imply that $\mathbf{B_0}$ is nonempty**,** so all that remains is to verify that $\mathbf{B_0}$ contains more than its least element**.** In fact**,** if **m** is the least element and **z > m,** then we claim that $\mathbf{x \in B_0}$**,** for otherwise we would have **z ∈ C,** and therefore the third property would imply **m ∈ C,** which we know is false**.**

We shall now verify the three characterizing properties in order. **(1)** Observe that if **y** is any element of **C** then **y** is a lower bound for the sets $\mathbf{B_0}$ and **B;** to see this, suppose that $\mathbf{x \in B_0}$ and that **y** is not strictly less than **x.** Then we have **x ≤ y,** and by the defining properties of **C** it will follow that **x ∈ C,** which contradicts the construction of $\mathbf{B_0}$ as a set that is disjoint from **C.** It therefore follows that **– y** is an upper bound for **– C. (2)** For each **x ∈ – C** we need to find some **y** such that **y ∈ – C** and **y > x.** By definition**,** if we have **x ∈ – C** then $\mathbf{-x \in B_0}$ but **– x** is not the least element of the latter**.** If $\mathbf{B_0}$ has no least element then clearly there is some **w ∈ B** such that **w < – x.** If $\mathbf{B_0}$ has a least element we have to look more carefully**.** Suppose that **w** lies between the least element **m** and **– x;** we claim that **w ∈ B.** If not**,** then **w ∈ C,** and by the third condition in the definition of a left Dedekind set it will follow that **m ∈ C,** which is false**.** Therefore in both cases we have an element of **B** such that **w < – x,** and hence we also have **x < – w** where both of the latter belong to **– C.** Therefore the latter set has no largest element**.** **(3)** If **x < y** and **y ∈ – C,** then we need to prove that **x ∈ – C.** By construction we know that **– y ∈ B,** and of course we also have **– y < – x,** so the proof reduces to showing that **– x ∈ B.** What are the other possibilities? One option is that **– x** could be the least element of $\mathbf{B_0}$**,** but this is not true because it is greater than **– y** and the latter lies in **B.** Thus the only remaining alternative to **– x ∈ B** is that we have **– x ∈ C.** Since **– x > – y** it would follow that **– y** would lie in **C** and we know this is false because **– y** actually lies in the disjoint subset **B.** Therefore the only possibility is that **– x ∈ B,** which is equivalent to **x ∈ – C.** *This completes the proof that the set* **– C** *is a left Dedekind set.*■

The general definition of multiplication is more complicated. However, if we are given two sets **C** and **D** that are ***positive*** in the sense that both contain **0** (hence also contain some positive rational numbers), the definition is again simple**:** The *product* of the sets **C·D** is then taken to be the set of all rational numbers expressible as **x·y** where **x ∈ C** and **y ∈ D.** In the remaining cases one must adjust the definition**;** this is explained thoroughly on page 15 of Goldrei**,** and it simply corresponds to the usual rules for determining whether the product of two numbers is positive**,** negative or zero if at least one of the factors is nonpositive**.** We specifically took the trouble to define the negative

of a left Dedekind set explicitly so that the notion could be used in the definition of multiplication.

Having defined the algebraic structure on left Dedekind sets, it remains to verify that the ordering and algebraic operations satisfy all the properties that are supposed to hold for the real numbers. These are listed in Theorem 2.3 on page 16 of Goldrei. Once again, the first online document cited above has all the details.

The Cantor construction of the real numbers

Given the fundamental importance of the real numbers in mathematics, it certainly would not hurt to confirm the existence of such a system by describing another construction. The standard alternative to Dedekind's construction is the so – called ***Cauchy sequence construction*** due to Cantor. Both yield systems satisfying the axioms for the real numbers, and by the uniqueness results in Section 3, the systems obtained by the different methods are the same for all mathematical purposes. Each approach to constructing the real number system has its own advantages and disadvantages. Some constructions or proofs that are simple and natural in one are difficult or awkward in the other. In particular, the definition of multiplication is much easier in Cantor's construction, but one does not need to worry about equivalence classes in Dedekind's construction, which defines real numbers directly as subsets of the rationals.

The starting point for Cantor's construction is slightly different to the basic idea exploited by Dedekind; namely, *every real number is the limit of a sequence of rational numbers*. There are several ways one can see this, and the standard representations by (usually) unending decimal expansions provide a particularly direct means of doing so (see Section **V.5** of these notes).

Cantor's construction of the real numbers is described on pages 17 – 24 of Goldrei. In order to begin, one needs to define a type of sequence that looks like it should have a limit; the precise concept is called a ***Cauchy sequence***, and it is defined on page 18 (***Note:*** On page 17, Goldrei notes that every Cauchy sequence of real numbers converges to a limit and describes this as "a dull observation" — not everyone would agree with this opinion, and regardless of whether or not one agrees with it, the result itself and its numerous generalizations are extremely important for many purposes). Sequences whose values are constant and equal to some fixed rational number are Cauchy sequences, and they yield an embedding of the rationals into the set of equivalence classes of Cauchy sequences. One then defines a notion of equivalence if the sequences approach each other asymptotically, after which one defines addition, multiplication and ordering as on pages 22 – 23 of Goldrei. It follows immediately that these operations correspond to the ones we already have for rational numbers. Finally, as indicated on page 23 of Goldrei, one proves that the sets of equivalence classes of Cauchy sequences have all the required properties of the real number system, and this completes the proof that Cantor's construction also yields a model for the real numbers.

The preceding discussions of the Dedekind and Cantor constructions of the real numbers are only meant to summarize the latter and to indicate the crucial role of infinite set theory in both approaches. A reader interested in seeing more of the details is urged to consult the listed references.

The roles of the real number constructions

Most books on the theory of functions of a real variable written during the past few decades begin with the axioms for the real number system and proceed to develop the foundations of calculus from that basis. The actual means of construction of the real numbers is unimportant from this viewpoint, and the following quote from page 16 of Goldrei summarizes the situation quite well:

> The methods found in standard real analysis texts ... never "look inside" any real number, so the fact that a real number has been defined as a set of rationals ceases to be relevant.

Although the method of construction for the real numbers is relatively unimportant once the process is finished, both the Dedekind and Cantor methods are useful for studying certain other types of questions about embedding one mathematical system in another, where the latter has some desired properties; usually these involve adjoining additional points so that certain "good" sequences will have limits. Such constructions occur frequently in mathematics and its applications (particularly to physics), and they are characterized by names such as ***envelopes, extensions, compactifications, limiting objects,*** or (the default term) ***completions.***

We conclude this discussion of the real numbers with another quotation taken from pages 16 – 17 of Goldrei, which summarizes the preceding discussion and relates it to the material at the end of Section **V.2:**

> It is relevant to note at what cost we have defined the real numbers. First, we have defined reals in terms of rational numbers. ... Secondly, the definition of an individual real number is as an infinite set of rationals. Use of the infinite in mathematics has been a matter of controversy for a good 2000 [*actually, more like 2500*] years [*in* ***Western*** *civilization at least – many classical Indian mathematicians were not at all reluctant to discuss such matters*]. Arguably mathematicians of the 19th century were confident with what is called a ***potentially*** infinite set, one for which, however (finitely) many elements you have, there is always another available. But in treating an ***actually*** infinite set, like a Dedekind left set of rationals, as a legitimate mathematical object suitable for all sorts of manipulation, seemed somewhat dubious.

Complex numbers and other standard constructions. Once the real numbers are defined, there is no problem defining systems like the complex numbers, the usual coordinate spaces of n – dimensional vectors with real or complex coefficients, or any of the other objects one sees in basic undergraduate mathematics; in fact, all the usual construction go through unchanged.

VIII. 3 : Uniqueness of number systems

In the preceding section we outlined the construction of number systems which satisfy the basic properties of the integers, rational numbers and real numbers using the Standard Axiom of Infinity. The purpose of this section is to provide detailed proof of the following uniqueness results for number systems from Unit **V:**

Theorem V.1.6. *Suppose that* **X** *and* **Y** *are sets with notions of addition, multiplication and ordering which satisfy all the conditions for the integers. Then there exists a* ***unique*** $\mathbf{1-1}$ *correspondence from* **h** *from* **X** *to* **Y** *that is an* ***isomorphism*** *in the appropriate sense*: *For all* $\mathbf{u, v \in X}$ *we have* $\mathbf{h(u+v) = h(u) + h(v)}$, $\mathbf{h(u \cdot v) = h(u) \cdot h(v)}$, *and* $\mathbf{h(u) < h(v)}$ *if and only if* $\mathbf{u < v}$. *The map* **h** *sends the zero and unit of* **X** *to the zero and unit of* **Y** *respectively*.

Theorem V. 4.4. *Suppose that* **X** *and* **Y** *are sets with notions of addition, multiplication and ordering which satisfy all the conditions for the real number system. Then there exists a* ***unique*** $\mathbf{1-1}$ *correspondence from* **h** *from* **X** *to* **Y** *that is an* ***isomorphism*** *in the same sense as above*: *For all* $\mathbf{u, v \in X}$ *we have* $\mathbf{h(u+v) = h(u) + h(v)}$, $\mathbf{h(u \cdot v) = h(u) \cdot h(v)}$, *and* $\mathbf{h(u) < h(v)}$ *if and only if* $\mathbf{u < v}$. *The map* **h** *sends the zero and unit of* **X** *to the zero and unit of* **Y**, *and accordingly it also sends the "integers" in* **X** *to the "integers" in* **Y** *(and similarly for the "rationals" in the appropriate systems).*

As indicated in Unit **V**, these results imply that

> ***any mathematical statement about the addition, multiplication and ordering of* X *is true about the addition, multiplication and ordering of* Y *and conversely.***

Informally, this means that **X** and **Y** are "***the same for all practical purposes.***" The significance of this is also noted in Sections **V.1** and **V.4;** if there are two systems that satisfy these axioms such that the properties of addition, multiplication and ordering differed in some nontrivial fashion, then one can and should question ***whether there are different versions of mathematics depending upon which system of is chosen to be the* "integers" *or the* "real numbers."** The uniqueness theorem implies that no such difficulties of this sort exist.

Existence of an isomorphism

As usual with statements about the existence of a unique object, the proof splits into two parts, one to establish existence and the other to establish uniqueness. Therefore our first objective will be to construct an isomorphism from **X** to **Y.** We shall start very formally and write our systems as $\mathbf{(X, A_X, M_X, O_X)}$ and $\mathbf{(Y, A_Y, M_Y, O_Y)}$, where **A** and **M** denote the respective additions and multiplications and **O** denotes the respective linear orderings. In this terminology, an isomorphism from **X** to **Y** will denote a $\mathbf{1-1}$ correspondence $\mathbf{f: X \to Y}$ such that for all $\mathbf{u, v \in X}$ we have the following relations:

(1) $\mathbf{f(A_X(u, v)) = A_Y(f(u), f(v))}$. [The mapping **f** is ***additive***.]

(2) $\mathbf{f(M_X(u, v)) = M_Y(f(u), f(v))}$. [The mapping **f** is ***multiplicative***.]

(3) If $\mathbf{(u, v) \in O_X}$, then $\mathbf{(f(u), f(v)) \in O_Y}$. [The mapping **f** is ***order preserving***.]

Formally, we want to prove the following.

Theorem 1. *If* **X** *and* **Y** *are systems satisfying the axioms for either the integers or the real numbers (the same number system in both cases), then there exists an isomorphism* $\mathbf{f: X \to Y}$ *in the sense described above.*

It is an elementary exercise to verify that if **f** defines an isomorphism from **X** to **Y,** then the inverse function $\mathbf{f}^{-1}$ defines an isomorphism from **Y** to **X.** In particular**,** if **X** is isomorphic to **Y,** then **Y** is isomorphic to **X** and one can simply say that **X *and* Y *are isomorphic*** (to each other)**.**

The constructions of the isomorphisms start with the definition for natural numbers (**=** nonnegative integers) and the proceeds to its definition for the (signed) integers**;** in the case of the real numbers**,** the definition is extended still further**,** first to the rational numbers and ultimately to the real numbers**.** The first step in both arguments is the same**.**

First step. We have already noted that there are (unique) embeddings of the natural numbers — say $\mathbf{e_X}$ and $\mathbf{e_Y}$ — into **X** and **Y** sending zero element $\mathbf{0}$ of $\mathbb{N}$ to the zero elements $\mathbf{0_X}$ and $\mathbf{0_Y}$ of **X** and **Y** respectively and satisfying the basic conditions

$$\mathbf{e_X(\sigma(n))} \;=\; \mathbf{e_X(n)} \;+\; \mathbf{1_X}\,, \quad \mathbf{e_Y(\sigma(n))} \;=\; \mathbf{e_Y(n)} \;+\; \mathbf{1_Y}$$

where $\mathbf{1_X}$ and $\mathbf{1_Y}$ are the unit elements of **X** and **Y** respectively**.** For each $\mathbf{x \in X}$ there is at most one $\mathbf{n \in \mathbb{N}}$ such that $\mathbf{x = e_X(n)}$**,** and therefore we can construct a well – defined function

$$\mathbf{f_1 : e_X[\mathbb{N}] \to e_Y[\mathbb{N}]}$$

by setting $\mathbf{f_1(e_X(n)) = e_Y(n)}$ for $\mathbf{n \in \mathbb{N}}$**.** By construction this defines a one-to-one correspondence between $\mathbf{e_X[\mathbb{N}]}$ and $\mathbf{e_Y[\mathbb{N}]}$**.**

CLAIM*:* The map $\mathbf{f_1}$ satisfies the conditions

$$\mathbf{f_1(A_X(u, v)) \;=\; A_Y(f_1(u), f_1(v))},$$

$$\mathbf{f_1(M_X(u, v)) \;=\; M_Y(f_1(u), f_1(v))},$$

$$\text{if } \mathbf{(u, v) \in O_X}, \text{ then } \mathbf{(f_1(u), f_1(v)) \in O_Y}$$

for all $\mathbf{u, v \in \mathbb{N}}$**.** Using the maps $\mathbf{e_X}$ and $\mathbf{e_Y}$ we may rewrite these conditions as

$$\mathbf{f_1(A_X(e_X(m), e_X(n))) \;=\; A_Y(f_1(e_X(m)), f_1(e_X(n)))},$$

$$\mathbf{f_1(M_X(e_X(m), e_X(n))) \;=\; M_Y(f_1(e_X(m)), f_1(e_X(n)))},$$

$$\mathbf{\text{if } (e_X(m), e_X(n)) \in O_X, \text{ then } (f_1(e_X(m)),\; f_1(e_X(n))) \in O_Y}$$

for all $\mathbf{m, n \in \mathbb{N}}$**.** We shall verify the first two of these by induction on **n;** in order to simplify the notation and stress the underlying ideas we shall use the standard algebraic terminology to denote the addition**,** multiplication and linear orderings on **X** and **Y.**

Addition. Suppose that $\mathbf{n = 0}$**.** Then

$$\mathbf{f_1(e_X(m) + e_X(0)) \;=\; f_1(e_X(m) + 0_X) \;=\; f_1(e_X(m)) \;=}$$
$$\mathbf{e_Y(m) + 0_Y \;=\; e_Y(m) + e_Y(0) \;=\; f_1(e_X(m)) + f_1(e_X(0))}.$$

Thus the equation is true for $\mathbf{n = 0}$ and all **m.** Suppose now that it is true for $\mathbf{n = k}$ and all **m;** we need to show it is true for $\mathbf{n = \sigma(k)}$ and all **m.** But

$$\mathbf{f_1(e_X(m) + e_X(\sigma(k))) \;=\; f_1(e_X(m) + e_X(k) + 1_X) \;=\; f_1(e_X(m) + e_X(k) + 1_X) \;=}$$
$$\mathbf{f_1(e_X(m) + 1_X + e_X(k)) \;=\; f_1(e_X(\sigma(m)) + e_X(k))}$$

and by the induction hypothesis the last expression is equal to

$$f_1(e_X(\sigma(m))) + f_1(e_X(k)).$$

The latter in turn is equal to

$$e_Y(\sigma(m)) + e_Y(k) = e_Y(m) + 1_Y + e_Y(k) = e_Y(m) + e_Y(\sigma(k)) = f_1(e_X(m)) + f_1(e_X(\sigma(k))).$$

This completes the verification of the inductive step.

Multiplication. Suppose that $n = 0$. Then

$$f_1(e_X(m)\cdot e_X(0)) = f_1(e_X(m)\cdot 0_X) = f_1(0_X) = 0_Y = e_Y(m)\cdot 0_Y = e_Y(m)\cdot e_Y(0) = f_1(e_X(m))\cdot f_1(e_X(0)).$$

Thus the equation is true for $n = 0$ and all m. Suppose that we know the equation is true for $n = k$ and all m; we need to show it is true for $n = \sigma(k)$ and all m. But

$$f_1(e_X(m)\cdot e_X(\sigma(k))) = f_1(e_X(m)\cdot e_X(k) + e_X(m)) = f_1(e_X(m)\cdot e_X(k)) + f_1(e_X(m))$$

because we have already verified that f_1 is additive, and by the induction hypothesis the last expression is equal to $f_1(e_X(m))\cdot f_1(e_X(k)) + f_1(e_X(m))$. The latter in turn is equal to

$$e_Y(m)\cdot e_Y(k) + e_Y(m) = e_Y(m)\cdot e_Y(\sigma(k)) = f_1(e_X(m))\cdot f_1(e_X(\sigma(k))).$$

As before, this completes the verification of the inductive step.

Ordering. If $e_X(m) < e_X(n)$ then there is a nonzero natural number $c \in \mathbb{N}$ such that $e_X(m) + e_X(c) = e_X(n)$. Since f_1 is one-to-one, it follows that $e_Y(c) = f_1(e_X(c)) \neq 0_Y$, so that $e_Y(c) > 0_Y$. By the additivity of f_1 it follows that

$$f_1(e_X(m)) = e_Y(m) = e_Y(m) + 0_Y < e_Y(m) + e_Y(c) = f_1(e_X(m) + e_X(c)) = f_1(e_X(n))$$

as required.

Notational conventions. Let F be a system satisfying the axioms for the integers or the real number system, and let $e_F : \mathbb{N} \to F$ be the embedding of the natural numbers that has been used extensively in the preceding step of the proof. We define the **integers** in F to be the set of all objects of the form $e_F(a) - e_F(b)$ for some $a, b \in \mathbb{N}$, and we shall denote this set by $\mathbb{Z}(F)$. Similarly, if F satisfies the axioms for the reals, we define the ***rational numbers*** or ***rationals*** in F to be the set of m/n where m and n are integers in F and n is nonzero, and we shall denote this set by $\mathbb{Q}(F)$. If we are dealing with one fixed system in a given context we shall omit the "(F)" to simplify and standardize the notation.

Second step. We need to extend f_1 to negative integers. Clearly we want a definition sending a negative number of the form $-e_X(n) \in X$ to $-e_Y(n) = -f_1(e_Y(n))$, but we shall take a slightly less direct approach that will be helpful in verifying the crucial properties of the extended map without a succession of case by case arguments.

By the preceding definition, every integer $\mathbf{n} \in \mathbf{X}$ can be represented as a difference $\mathbf{e_X(a) - e_X(b)}$ for some $\mathbf{a, b} \in \mathbb{N}$; this representation is not unique, but it is elementary to check that $\mathbf{e_X(a) - e_X(b) = e_X(c) - e_X(d)}$ if and only if

$$\mathbf{e_X(a) + e_X(d) = e_X(b) + e_X(c).}$$

We shall extend $\mathbf{f_1}$ to a map $\mathbf{f_2}$ on integers by setting

$$\mathbf{f_2\,(e_X(a) - e_X(b)) = e_Y(a) - e_Y(b) = f_1(e_X(a)) - f_1(e_X(b)).}$$

Before proceeding any further we need to show that $\mathbf{f_2}$ is well-defined; in other words, we need to verify that

$$\text{if } \mathbf{e_X(a) - e_X(b) = e_X(c) - e_X(d),} \text{ then } \mathbf{e_Y(a) - e_Y(b) = e_Y(c) - e_Y(d).}$$

Equivalently, we need to show that

$$\text{if } \mathbf{e_X(a) + e_X(d) = e_X(b) + e_X(c),} \text{ then } \mathbf{e_Y(a) + e_Y(d) = e_Y(b) + e_Y(c).}$$

To see the latter, apply $\mathbf{f_1}$ to both sides of the first equation and note that the additivity of $\mathbf{f_1}$ on $\mathbb{N}$ implies that

$$\mathbf{e_Y(a) + e_Y(d) = f_1(e_X(a)) + f_1(e_X(d)) = f_1(e_X(a) + e_X(d)) =}$$
$$\mathbf{f_1(e_X(b) + e_X(c)) = f_1(e_X(b)) + f_1(e_X(c)) = e_Y(b) + e_Y(c)}$$

so that $\mathbf{f_2}$ is well-defined.

Throughout the remainder of this step in the proof we shall consider two integers in $\mathbf{X}$ of the form $\mathbf{m = e_X(a) - e_X(b)}$ and $\mathbf{n = e_X(c) - e_X(d).}$

We must now show that $\mathbf{f_2}$ is $\mathbf{1-1.}$ To see this, suppose that $\mathbf{f_2(m) = f_2(n).}$ By construction it follows that $\mathbf{e_Y(a) - e_Y(b) = e_Y(c) - e_Y(d)}$ so that we have $\mathbf{e_Y(a) + e_Y(d) = e_Y(b) + e_Y(c).}$ The identities of the previous paragraph now imply that

$$\mathbf{f_1(e_X(a) + e_X(d)) = f_1(e_X(b) + e_X(c))}$$

and since $\mathbf{f_1}$ is $\mathbf{1-1}$ it follows that $\mathbf{e_X(a) + e_X(d) = e_X(b) + e_X(c).}$ But the latter implies $\mathbf{e_X(a) - e_X(b) = e_X(c) - e_X(d)}$ which in turn implies that $\mathbf{m = n.}$ By construction it follows that the image of $\mathbf{f_2}$ is the set of all differences of elements in the image of $\mathbf{e_Y}$; in other words, $\mathbf{f_2}$ ***maps the integers in*** $\mathbf{X}$ ***onto the integers in*** $\mathbf{Y.}$

We next verify that $\mathbf{f_2}$ is additive:

$$\mathbf{f_2(m + n) = f_2(e_X(a) - e_X(b) + e_X(c) - e_X(d)) =}$$
$$\mathbf{f_2\,(e_X(a) + e_X(c) - e_X(b) - e_X(d)) = f_2\,((e_X(a) + e_X(c)) - (e_X(b) + e_X(d))) =}$$
$$\mathbf{f_1(e_X(a) + e_X(c)) - f_1(e_X(b) + e_X(d)) = (e_Y(a) + e_Y(c)) - (e_Y(b) + e_Y(d)) =}$$
$$\mathbf{e_Y(a) - e_Y(b) + e_Y(c) - e_Y(d) = f_2(m) + f_2(n).}$$

The verification that $\mathbf{f_2}$ is multiplicative proceeds similarly:

$$\mathbf{f_2(m \cdot n) = f_2\,((e_X(a) - e_X(b)) \cdot (e_X(c) - e_X(d))) =}$$
$$\mathbf{f_2((e_X(a) \cdot e_X(c) + e_X(b) \cdot e_X(d)) - (e_X(a) \cdot e_X(d) + e_X(b) \cdot e_X(c))) =}$$
$$\mathbf{f_1(e_X(a) \cdot e_X(c) + e_X(b) \cdot e_X(d)) - f_1(e_X(a) \cdot e_X(d) + e_X(b) \cdot e_X(c)) =}$$
$$\mathbf{(f_1(e_X(a)) \cdot f_1(e_X(c)) + f_1(e_X(b)) \cdot f_1(e_X(d))) -}$$
$$\mathbf{(f_1(e_X(a)) \cdot f_1(e_X(d)) + f_1(e_X(b)) \cdot f_1(e_X(c))) =}$$

$$(e_Y(a)\cdot e_Y(c) + e_Y(b)\cdot e_Y(d)) - (e_Y(a)\cdot e_Y(d) + e_Y(b)\cdot e_Y(c)) =$$
$$(e_Y(a) - e_Y(b))\cdot(e_Y(c) - e_Y(d)) = f_2(m)\cdot f_2(n).$$

To prove that f_2 is order preserving, suppose that $m < n$, so that we have

$$e_X(a) - e_X(b) < e_X(c) - e_X(d).$$

Adding $e_X(b) - e_X(d)$ to both sides of this inequality yields

$$e_X(a) + e_X(d) < e_X(b) + e_X(c)$$

and since f_1 is order preserving the latter in turn implies

$$e_Y(a) + e_Y(d) = f_1(e_X(a)) + f_1(e_X(d)) = f_1(e_X(a) + e_X(d)) <$$
$$f_1(e_X(b) + e_X(c)) = f_1(e_X(b)) + f_1(e_X(c)) = e_Y(a) + e_Y(c).$$

If we now subtract $e_Y(b) + e_Y(d)$ from both sides of the outside inequality we obtain the desired conclusion:

$$f_2(m) = e_Y(a) - e_Y(b) < e_Y(c) - e_Y(d) = f_2(n)$$

This completes the second step of the proof.

Note that the preceding two steps complete the proof of Theorem **V.1.6.**■

Third step. We may now assume that **X** and **Y** satisfy the axioms for the real numbers, so that we need an extension of f_2 to rational numbers of the form a/b where **a** and **b** are integers and **b** is nonzero. Recall from elementary algebra that two fractions a/b and c/d (with **b** and **d** nonzero) are equal if and only if $ad = bc$.

The idea is to consider a number $q \in X$ of the form a/b, where **a** and **b** are integers in **X** and **b** is nonzero, and to define $f_3(q) = f_2(a)/f_2(b)$. In order to show that this is a valid definition we need to check two things. First of all, since f_2 is $1-1$ it follows that $f_2(b)$ is nonzero if **b** is nonzero, so the quotient is actually defined. Second, we need to show that the value obtained by the formula is the same if we write **q** as a quotient of integers in two different ways. In other words, we need to show that if $a/b = c/d$ (with **b** and **d** nonzero) then we also have $f_2(a)/f_2(b) = f_2(c)/f_2(d)$. To do this, begin with the previous observation that $ad = bc$ and apply f_2 to both sides of the equation to obtain $f_2(a)\cdot f_2(d) = f_2(b)\cdot f_2(c)$. If we then divide both sides of this equation by $f_2(b)\cdot f_2(d)$ we obtain the desired equation $f_2(a)/f_2(b) = f_2(c)/f_2(d)$.

By construction the image of f_3 consists of all expressions of the form u/v where **u** and **v** are in the image of f_2 and **v** is nonzero; in other words, f_3 **maps the rationals in X onto the rationals in Y.** We claim that f_3 is also $1-1$.

Throughout the remainder of this step in the proof we shall consider two rational numbers in **X** of the form $p = a/b$ and $q = c/d$ where **a, b, c, d** are integers in **X** and **b** and **d** are nonzero.

To prove that f_3 is $1-1$, suppose that $f_3(p) = f_3(q)$. By construction it follows that $f_2(a)/f_2(b) = f_2(c)/f_2(d)$, which is equivalent to $f_2(a)\cdot f_2(d) = f_2(b)\cdot f_2(c)$. Since f_2 is multiplicative we have $f_2(ad) = f_2(a)\cdot f_2(d) = f_2(b)\cdot f_2(c) = f_2(bc)$, and since f_2 is one-to-one this implies $ad = bc$, which in turn implies $a/b = c/d$ and hence that ***the mapping*** f_3 ***is also*** $1-1$.

The ***verification that*** $\mathbf{f_3}$ ***is additive*** is a consequence of the following string of equations:

$$f_3\left(\frac{a}{b}+\frac{c}{d}\right)=f_3\left(\frac{ad+bc}{bd}\right)=\frac{f_2(ad+bc)}{f_2(bd)}=\frac{f_2(a)f_2(d)+f_2(b)f_2(c)}{f_2(b)f_2(d)}=$$

$$\frac{f_2(a)}{f_2(b)}+\frac{f_2(c)}{f_2(d)}=f_3\left(\frac{a}{b}\right)+f_3\left(\frac{c}{d}\right).$$

Similarly, the ***verification that*** $\mathbf{f_3}$ ***is multiplicative*** follows from a somewhat different string of equations:

$$f_3\left(\frac{a}{b}\cdot\frac{c}{d}\right)=f_3\left(\frac{ac}{bd}\right)=\frac{f_2(ac)}{f_2(bd)}=\frac{f_2(a)f_2(c)}{f_2(b)f_2(d)}=$$

$$\frac{f_2(a)}{f_2(b)}\cdot\frac{f_2(c)}{f_2(d)}=f_3\left(\frac{a}{b}\right)\cdot f_3\left(\frac{c}{d}\right).$$

Finally we need to ***show that*** $\mathbf{f_3}$ ***is order preserving.*** We shall do this using the fact that a fraction $\mathbf{a/b}$ is positive if and only if the product of the number and denominator $\mathbf{ab}$ is positive (the second number is the product of the first with the positive number $\mathbf{b^2}$). Therefore suppose that $\mathbf{p < q}$; then $\mathbf{p - q}$ is positive, and by the observation on the signs of fractions in the previous sentence it follows that the integer $\mathbf{(bc - ad)\cdot bd}$ is also positive. Since $\mathbf{f_2}$ is order preserving it follows that

$$\mathbf{f_2((bc-ad)\cdot bd)=(f_2(b)\cdot f_2(c)-f_2(a)\cdot f_2(d))\cdot(f_2(b)\cdot f_2(d))}$$

is also positive. But the right hand side of this equation is equal to $\mathbf{f_3(q) - f_3(p)}$, so the preceding observations imply that $\mathbf{f_3(q) > f_3(p)}$ as required.

Fourth step. We need to extend $\mathbf{f_3}$ to all elements of $\mathbf{X}$. Given a number $\mathbf{r \in X}$, consider the set $\mathbf{D(r)}$ of all rational numbers $\mathbf{q \in X}$ such that $\mathbf{q < r}$. Let $\mathbf{k}$ be a positive integer that is greater than $\mathbf{r}$, and consider the set $\mathbf{f_3[D(r)] \subset Y}$. Since $\mathbf{f_3}$ is order preserving it follows that $\mathbf{f_3(k)}$ is an upper bound for $\mathbf{f_3[D(r)]}$ and therefore by completeness the set $\mathbf{f_3[D(r)]}$ has a (unique) least upper bound; we take $\mathbf{f(r)}$ to be this least upper bound. This definition may be rewritten as follows:

$$\mathbf{f(r) = L.U.B._{q<r}\ f_3(q)}$$

The first order of business is to show that $\mathbf{f_3(r) = f(r)}$ when $\mathbf{r}$ is rational. If $\mathbf{r}$ is rational and $\mathbf{q \in D(r)}$, then by the previous work we know that $\mathbf{f_3(q) < f_3(r)}$, so that $\mathbf{f_3(r)}$ is an upper bound for $\mathbf{f_3[D(r)]}$ and consequently is greater than or equal to the least upper bound, which is $\mathbf{f(r)}$. Suppose now that $\mathbf{f(r) < f_3(r)}$. It follows that there is a rational number $\mathbf{t \in X}$ such that $\mathbf{f(r) < f_3(t) < f_3(r)}$. Since $\mathbf{f_3}$ is order preserving, the second inequality implies that $\mathbf{t < r}$. The latter in turn implies $\mathbf{t \in D(r)}$ and hence $\mathbf{f_3(t) \leq f(r)}$, which when combined with the previously displayed inequality $\mathbf{f(r) < f_3(t)}$ yields a contradiction. It follows that $\mathbf{f(r) = f_3(r)}$.

To ***show that*** $\mathbf{f}$ ***is*** $\mathbf{1-1}$, assume that $\mathbf{r}$ and $\mathbf{s}$ are real numbers in $\mathbf{X}$ such that $\mathbf{r < s}$. Choose rational numbers $\mathbf{p}$ and $\mathbf{q}$ such that $\mathbf{r < p < q < s}$. As before, it follows that $\mathbf{f_3(p)}$ is an upper bound for $\mathbf{f_3[D(r)]}$ and therefore we have $\mathbf{f(r) \leq f_3(p) = f(p)}$. Furthermore, since $\mathbf{f_3 = f}$ for rational numbers it follows that $\mathbf{f(p) < f(q)}$, and also since

$q \in D(s)$ it follows that $f(q) = f_3(q) \leq f(s)$. If we put these inequalities together we find that $f(r) < f(s)$ and consequently that f ***is also*** $1-1$. Note that ***this argument also shows that*** f ***is order preserving.***

We shall next ***verify that the function*** f ***maps*** X ***onto all of*** Y. Let $y \in Y$ be arbitrary, and let $D^*(y)$ be the set of all rational numbers $q \in Y$ such that $q < y$; by construction y is an upper bound for $D^*(y)$, and in fact the least upper bound of $D^*(y)$ is equal to y because if $z < y$ then there is a rational number p such that $z < p < y$. As before there is a positive integer $k \in Y$ such that $y < k$, and since the function f_3 is order preserving it follows that $k_0 = f_3^{-1}(k)$ is an upper bound for the set $f_3^{-1}[D^*(y)]$. Therefore the latter set has an upper bound that we shall denote by x. We claim that $f(x) = y$, and we shall do this by showing that $y \leq f(x)$ and strict inequality does not hold. To show the inequality, suppose that we have $q < y$, and choose a rational number $p \in Y$ such that $q < p < y$. If we write $q_0 = f_3^{-1}(q)$ and $p_0 = f_3^{-1}(p)$, then $q_0 < p_0$, and since both belong to the set $f_3^{-1}[D^*(y)]$ it follows that $q_0 < p_0 < x$. Since the function f is order preserving the identities $p = f_3(p_0) = f(p_0)$ and $q = f_3(q_0) = f(q_0)$ imply the chain of inequalities $q < p < f(x)$. Thus $f(x)$ is an upper bound for $D^*(y)$; since y is the least upper bound for $D^*(y)$, we must have $y \leq f(x)$. The proof that $y = f(x)$ thus reduces to showing that $f(x)$ is ***not*** strictly greater than y.

Assume the contrary. Then there is a rational number q satisfying $y < q < f(x)$, and write $q = f_3(q_0) = f(q_0)$ as before. Since the function f is order preserving, it follows that $q_0 < x$. But the definition of x as a least upper bound implies the existence of a rational number p_0 such that $q_0 < p_0$ and $p = f_3^{-1}(p_0)$ lies in $D^*(y)$; ***i.e.***, we must have $p < y$. Once again we have $q = f_3(q_0) < f_3(p_0) = p$, and if we combine this with the other inequalities, we get the longer string of inequalities $y < q < p < y$, which is a contradiction. This completes the proof that $y = f(x)$.

The next step is to ***show that*** f ***is additive.*** Let u and v be arbitrary real numbers in X.

Consider first the special case where one of these numbers (say v) is rational. In this case the set $D(u + v)$ is the set of all numbers expressible as sums

$$f_3(q) + f_3(v) = f_3(q) + f(v)$$

where $q \in D(u)$, and therefore we have

$$f(u + v) = \text{L.U.B.}_{q < u + v}\ f_3(q) = \left[\text{L.U.B.}_{p < u}\ f_3(p)\right] + f(v) = f(u) + f(v)$$

and hence f is additive if v is rational and u is arbitrary.

We now consider the general case. If q is a rational number such that $q < v$, then we have $f(u) + f(q) = f(u + q) < f(u + v)$ because f is order preserving and it is also additive if one of the summands is rational. Therefore $q < v$ implies that

$$f_3(q) = f(q) < f(u + v) - f(u)$$

and consequently we have

$$f(v) = \text{L.U.B.}_{q < v}\ f_3(q) \leq f(u + v) - f(u).$$

Additivity will follow if we can show that $f(v) < f(u + v) - f(u)$ is impossible, so assume that it does hold. In this case there is a rational number $r \in Y$ such that

$$f(v) < r < f(u+v) - f(u)$$

and because **f** is onto we may write $r = f(q)$ for some rational number $q \in X$. Since **f** is order preserving we know that $v < q$, and consequently the order preserving and partial additivity properties of **f** imply that

$$f(q) = r < f(u+v) - f(u) < f(u+q) - f(u) = f(u) + f(q) - f(u) = f(q)$$

which is a contradiction. Therefore the assumption $f(v) < f(u+v) - f(u)$ must be incorrect, and by the preceding discussion it follows that **f** must be additive.

At this point, ***the only statement that remains to be shown is that*** **f** **is multiplicative.** We first observe that **f** is multiplicative if at least one of the factors is 0 or ± 1. If one of the factors is $+1$, this is immediate because $f(1_X) = 1_Y$. If one of the factors is zero, this follows quickly because the product of anything with zero is zero and $f(0_X) = 0_Y$. If one of the factors is -1, this will follow provided we can demonstrate that $f(-a) = -f(a)$ for all $a \in X$, for then we have $f(-1_X) = -f(1_X) = -1_Y$ and furthermore

$$f((-1_X)\cdot a) = f(-a) = -f(a) = (-1_Y)\cdot f(a) = f(-1_X)\cdot f(a).$$

To see that $f(-a) = -f(a)$, let $b = -a$. Since **f** is additive we have that

$$0_Y = f(0_X) = f(a+b) = f(a) + f(b)$$

and the latter implies that $f(b) = -f(a)$ as required. We are going to need the basic identity $f(-a) = -f(a)$ in order to complete the final step in the verification that **f** is multiplicative.

The next step in verifying that **f** ***is multiplicative is to show this is true if both of the factors are positive.*** The proof of this fact is very similar to the proof of additivity (since the exponential map defines an order preserving isomorphism from the additive group of real numbers to the multiplicative group of positive real numbers, this should not be surprising). Let **u** and **v** be arbitrary ***positive*** real numbers in **X**. Since **f** is order and zero preserving it follows that both $f(u)$ and $f(v)$ are positive.

Consider first the special case where one of these numbers (say **v**) is rational (and positive!). In this case, the set $D(u\cdot v)$ is the set of all real numbers expressible as sums $f_3(q)\cdot f_3(v) = f_3(q)\cdot f(v)$ where $q \in D(u)$, and therefore we have

$$f(u\cdot v) = \text{L.U.B.}_{\,q < u\cdot v}\ f_3(q) = [\text{L.U.B.}_{\,p < u}\ f_3(p)]\cdot f(v) = f(u)\cdot f(v)$$

and hence **f** is multiplicative if **v** is rational and **u** is arbitrary.

We now consider the general case. If **q** is a rational number such that $q < v$, then we have $f(u)\cdot f(q) = f(u\cdot q) < f(u\cdot v)$ because **f** is order preserving and it is also additive if one of the summands is rational. Therefore $q < v$ implies that

$$f_3(q) = f(q) < f(u\cdot v)/f(u)$$

and consequently we have

$$f(v) = \text{L.U.B.}_{\,q < v}\ f_3(q) \le f(u\cdot v)/f(u).$$

Multiplicativity will follow if we can show that $f(v) < f(u\cdot v)/f(u)$ is impossible, so assume that it does hold. In this case there is a rational number $r \in Y$ such that

$$f(v) < r < f(u\cdot v)/f(u)$$

and because **f** is onto we may write **r = f(q)** for some rational number **q ∈ X.** Since **f** is order preserving we know that **v < q,** and consequently the order preserving and partial multiplicativity properties of **f** imply that

$$f(q) = r < f(u \cdot v)/f(u) < f(u \cdot q)/f(u) = f(u) \cdot f(q)/f(u) = f(q)$$

which is a contradiction. Therefore the assumption **f(v) < f(u · v)/f(u)** must be incorrect**,** and by the preceding discussion it follows that **f** must be multiplicative**.**

Finally**,** ***we need to verify that*** **f** ***is multiplicative in all cases.*** Given a nonzero real number **a,** set **ε(a)** equal to $+1$ if **a** is positive and -1 if **a** is negative**.** Then we may express **a = ε(a) · |a|** where the absolute value **|a|** is positive**.** Using the multiplicativity of **f** for the product **|u|·|v|** and the identity **f(ε · a) = ε · f(a)** for **ε = ±1** we have

$$f(u \cdot v) = f((\varepsilon(u) \cdot |u|) \cdot (\varepsilon(v) \cdot |v|)) = f(\varepsilon(u) \cdot \varepsilon(v) \cdot |u| \cdot |v|) =$$

$$(\varepsilon(u) \cdot \varepsilon(v)) \cdot f(|u| \cdot |v|) = (\varepsilon(u) \cdot \varepsilon(v)) \cdot f(|u|) \cdot f(|v|) =$$

$$(\varepsilon(u) \cdot f(|u|)) \cdot (\varepsilon(v) \cdot f(|v|)) = (f(\varepsilon(u) \cdot |u|)) \cdot (f(\varepsilon(v) \cdot |v|)) = f(u) \cdot f(v)$$

and this completes the proof that **f** is multiplicative**.** As noted before**,** this completes the proof of Theorem 1 as well as Theorem **V.4.4.**■

Uniqueness of the isomorphisms

It turns out that the isomorphisms constructed above are **unique.** This is equivalent to saying that if **A** satisfies the axioms for the integers or the real numbers**,** then ***the only isomorphism of* A *with itself that preserves addition, multiplication and ordering is the identity.*** In fact**,** a slightly stronger result is true**.**

Theorem 2. *If* **A** *satisfies the axioms for the real numbers or the integers and the mapping* **f: A → A** *is a* $1-1$ *correspondence that is additive and multiplicative (but is not* ***assumed*** *to preserve the ordering), then* **f** *is the identity***.**

It is possible to define meaningful notions of isomorphism for many different classes of mathematical objects**.** If the domain and codomain of an isomorphism are the same, it is often called an ***automorphism.*** Given an object satisfying the axioms for the real number system**,** the identity map on that object is always an automorphism**,** and the main result above can be reformulated to state that for a system satisfying the axioms for the real number system there are no other automorphisms**.**

Example of a nontrivial automorphism. In contrast**,** there are some systems closely related to the real number systems that have nontrivial automorphisms. Perhaps the most important example is the field of ***complex numbers*** $\mathbb{C}$**.** Of course**,** this is the system one obtains from the real numbers by adding an element $\mathbf{i}$ that is supposed to be the square root of -1**.** A detailed account of the complex numbers is really beyond the scope of these notes**,** but the book by Birkhoff and MacLane covers the basics in a clear**,** concise and thorough manner**.** Here our interest lies with the ***complex conjugation mapping*** on complex numbers sending a complex number **z = a + bi** to its conjugate **χ(z) = z* = a − bi.** This is a $1-1$ correspondence because the identity **z = (z*)***

implies $\chi\chi = 1_{\mathbb{C}}$, so that χ is its own inverse, and χ is an automorphism because complex conjugation satisfies the following two elementary identities:

$$(z + w)^* = z^* + w^* \qquad (z \cdot w)^* = z^* \cdot w^*$$

For the sake of completeness we note that ***the set of all automorphisms of the complex numbers is*** **HUGE** (in fact, its cardinality is $2^{|\mathbb{C}|} > |\mathbb{C}|$), but conjugation is the only nontrivial automorphism that sends real numbers to themselves and it is also the only nontrivial one which defines a ***continuous*** mapping from $\mathbb{C}$ to itself.

Proof of Theorem 2. The proof begins with a couple of simple observations:

(a) *The only element* $u \in A$ *such that* $x \cdot u = x$ *for all* $x \in A$ *is the unit element.*

(b) *The only element* $z \in A$ *such that* $x \cdot z = z$ *for all* $x \in A$ *is the zero element.*

These follow because $u = 1 \cdot u = 1$ and $0 = 0 \cdot z = z$. Since f sends elements with properties **(a)** and **(b)** into elements with the corresponding properties, it follows that we must have $f(1) = 1$ and $f(0) = 0$.

We shall also need two other standard elementary properties of automorphisms (and isomorphisms):

(c) *For all* $x \in A$ *we have* $f(-x) = -f(x)$.

(d) *If* $A = \mathbb{R}$, *then for all nonzero* $x \in A$ *we have* $f(x^{-1}) = f(x)^{-1}$.

The proof of **(c)** is the same argument that was used in the uniqueness proof, and the proof of **(d)** is based upon similar considerations:

$$1 = f(1) = f(x\,x^{-1}) = f(x)\,f(x^{-1}) \quad \Rightarrow \quad f(x^{-1}) = f(x)^{-1}$$

The main idea behind the proof is to show successively that f must be the identity on each of the following:

1. The natural numbers.
2. The integers.
3. The rational numbers.
4. All real numbers.

If A is the integers, then only the first two steps are needed. Predictably, we take these steps in the order listed.

The natural numbers. Let $e : \mathbb{N} \to A$ be the embedding described in the section on axioms for the real numbers. We shall show that $f(e(n)) = e(n)$ by induction on n; we have already verified this if $n = 0$ or $n = 1$. Suppose that this is known for $n = k$. Then by the additivity of f and the inductive hypothesis we have

$$f(e(\sigma(k))) = f(e(k) + 1) = f(e(k)) + 1 = e(k) + 1 = e(\sigma(k)),$$

and hence f is the identity on the natural numbers (more correctly, on the image of the natural numbers in the reals).

The integers. Given an integer $n \in \mathbb{Z}$, write $n = e(a) - e(b)$ where $a, b \in \mathbb{N}$. Then by the preceding step in the proof, the additivity condition and property **(c)** above we have

$$f(n) = f(e(a) - e(b)) = f(e(a)) - f(e(b)) = e(a) - e(b) = n$$

as required. Note that ***this completes the proof if*** $A = \mathbb{Z}$.

The rational numbers. We may now assume that $A = \mathbb{R}$. Given an arbitrary rational number $q \in \mathbb{Q}$ express q as a quotient ab^{-1} where $a, b \in \mathbb{Z}$ and b is nonzero. As before, by the immediately preceding step in the proof, the multiplicativity of f and property **(d)** above we have

$$f(q) = f(ab^{-1}) = f(a)\,f(b^{-1}) = f(a)\,f(b)^{-1} = ab^{-1} = q$$

as required.

The set of all real numbers. The crucial step in the proof is to ***show that*** f ***is order preserving.*** Suppose that $a, b \in \mathbb{R}$ satisfy $a > b$. If $c = a - b$ then $c > 0$ and therefore c has a unique positive square root that we shall call d. If we apply f to both sides of the equation $d^2 = a - b$ we obtain the equation

$$f(d)^2 = f(d^2) = f(a - b) = f(a) - f(b);$$

this quantity is nonzero because f is $1 - 1$ (look at the right hand side), and it is nonnegative because it is a square (look at the left hand side). Therefore the quantity in question is positive as claimed.

To conclude the proof, let $a \in \mathbb{R}$ be arbitrary. We need to show that neither of the strict inequalities $a > f(a)$ or $a < f(a)$ can hold. The proofs in both cases are similar so we shall do them simultaneously. Suppose that $a > f(a)$ or $a < f(a)$ is true, and in the respective cases choose a rational number q such that

$$a > q > f(a) \quad \text{or} \quad a < q < f(a).$$

Since f is order preserving and is the identity on rational numbers, these inequalities respectively imply

$$f(a) > f(q) = q > f(a) \quad \text{and} \quad f(a) < f(q) = q < f(a).$$

In either case we obtain a contradiction, and therefore we must have $f(a) = a$. ■

VIII. 4 : Set theory and classical geometry

In Section **I.2** we noted that classical Euclidean geometry had served as a working foundation for much of mathematics before the development of set theory and the Dedekind – Cantor constructions for the real number system out of the rational numbers. Further discussion of this point appears on pages 212 and 258 – 259 of the following online documents:

http://math.ucr.edu/~res/math133/geomnotes5a.pdf

http://math.ucr.edu/~res/math133/geomnotes5b.pdf

We also noted in Section **I.2** that logical difficulties were noticed in the classical setting for geometry (***i.e.***, as presented in the ***Elements***) around the same time, but subsequent work near the end of the 19th century put classical geometry into a more logically rigorous form that meets current standards. The purpose of this appendix is to indicate in more detail how classical Euclidean geometry fits into the framework of set theory in modern mathematics. Our purpose is not really to go through the basics of classical Euclidean geometry but rather to explain how one integrates it into modern mathematics. References for further details will be given at appropriate points.

In the ***Elements,*** geometry is developed by starting with some basic assumptions on the properties of space and deriving an extensive list of logical consequences. If we are going to work within set theory, we must formulate the key mathematical aspects of geometry in set – theoretic terms rather than "physical reality." The first step in this process is very simple. A set should be a formal mathematical model for a geometrical plane or $\mathbf{3}$ – dimensional space $\mathbb{E}$, and the *points* of the space should be the elements of $\mathbb{E}$. The *lines*, and also the *planes* in the $\mathbf{3}$ – dimensional case, will then be sets of points and hence subsets of $\mathbb{E}$; the geometric concept of a point **x** lying on a line **L** or plane **P** will mean that **x** is an element of $\mathcal{L}$ or $\mathcal{P}$ respectively. In the ***Elements,*** both lines and planes are defined intuitively, but from the viewpoint of logic it is necessary to start with some things that are simply given without formal definitions, and therefore the formal set – theoretic approach to geometry takes lines and planes simply as distinguished classes of subsets, nothing more and nothing less. When we study geometry we usually think that these mathematical lines and planes should be idealizations of physical lines and planes, but this intuition serves only as a guide and motivation for our work. To summarize this discussion, the first steps in placing deductive geometry within the framework of set theory is to assume that plane or $\mathbf{3}$ – space of classical geometry should be a set $\mathbb{E}$, and the additional structure should one or two classes of proper subsets depending upon the dimension. In both cases there is a family of nonempty proper subsets $\mathcal{L}$ called ***lines,*** and in the $\mathbf{3}$ – dimensional case there is also a second family of nonempty proper subsets $\mathcal{P}$ called ***planes*** such that $\mathcal{L}$ and $\mathcal{P}$ are disjoint.

Clearly we need to make some assumptions about our undefined concdepts; for example, we obviously need to know that two points determining a unique line. Properties of this sort are called ***incidence axioms***, and here are lists of the respective axioms for the plane and $\mathbf{3}$ – space.

Planar axioms.

[**I – 1**] Given two distinct points **x** and **y** in $\mathbb{E}$, there is a unique line **L** in $\mathcal{L}$ such that both $\mathbf{x} \in \mathbf{L}$ and $\mathbf{y} \in \mathbf{L}$.

[**I – 2**] Every line **L** contains at least two points.

Spatial axioms. Add the following axioms to the previous ones:

[**I – 3**] Given three distinct points **x, y** and **z** in $\mathbb{E}$ such that no line **L** contains them all (***i.e.***, they are **noncollinear**), there is a unique plane **P** in $\mathcal{P}$ such that $\mathbf{x, y, z} \in \mathbf{L}$.

[**I – 4**] Every plane **P** contains at least three noncollinear points.

[**I – 5**] If two points of a line **L** belong to a plane **P**, then the entire line is contained in **P**.

[**I – 6**] If two planes have one point in common, then they also have a line in common.

The last two axioms correspond to everyday experience about the relation between planes and lines. One can derive various consequences from these assumptions (for example, that two distinct lines have at most one point in common), but we shall not work these out.

We now proceed to the basic measurement concepts in classical geometry; namely, linear and angular measurement. Once again, it is advisable to set things up formally so that at least linear measurement is an undefined concept and at this point it is also better to take both types of measurements as undefined concepts. We have mentioned that *the classical Greek approach to real numbers* was to *view them as lengths of segments*; we shall effectively reverse this approach by ***defining*** *lengths of segments in terms of the real number system*, which we now have at our disposal. Now the length of a segment can also be viewed as the distance between the endpoints, and the principle of Ockham's razor indicates the latter is preferable way of viewing an undefined concept because it will not require us to digress and explain exactly what a line segment should be. Therefore the "undefined" linear measurement structure will be a function

$$d : \mathbb{E} \times \mathbb{E} \rightarrow \mathbb{R}$$

that will have several properties, of which these are the most basic:

1. The quantity $d(\mathbf{x}, \mathbf{y})$ is always nonnegative, and it is zero if and only if $\mathbf{x} = \mathbf{y}$.
2. For all **x** and **y** we have $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$.

Likewise, at this point we would like to define angle measure in a manner that does not require us to explain exactly what is meant by an angle. Intuitively it is clear that a nontrivial angle (two distinct branch pieces and not a straight angle) is completely determined by 3 noncollinear points such that the middle one is the vertex of the angle. One way of doing this is to start by taking the subset $\mathit{Indep.}(\mathbb{E}\times\mathbb{E}\times\mathbb{E})$ of all ordered triples $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ in $\mathbb{E}\times\mathbb{E}\times\mathbb{E}$ such that **x**, **y** and **z** are three noncollinear points of $\mathbb{E}$ (*i.e.*, the three points are *geometrically independent*), and to define angle measurement to be a function

$$\alpha : \mathit{Indep.}(\mathbb{E}\times\mathbb{E}\times\mathbb{E}) \rightarrow (0, 180)$$

which will have some desired properties that we shall not attempt to describe for the time being.

Restriction to the planar case. Henceforth, unless there is an explicit statement to the contrary, we shall focus our attention on classical plane geometry. We have already seen that formulating incidence axioms is a somewhat more complicated in the $3-$ dimensional case. In fact, working everything out in three dimensions is a fairly routine extension of the $2-$ dimensional case; aside from the additional incidence axioms, it is only necessary to make some relatively straightforward adjustments in wording to a few of the axioms. This is not difficult, but the relatively minor differences make it awkward to discuss both cases simultaneously, and concentrating on the simpler case illustrates the basic ideas that arise in both situations.

By the preceding discussion, the data we need to discuss Euclidean plane geometry are the set $\mathbb{E}$ of points, the family $\mathcal{L}$ of lines, the linear measurement function d, and the angular measurement function α. Such an approach to axiomatic geometry is called a ***synthetic metric approach***. The idea is basically due to G. D. Birkhoff (1884 – 1944), and it is described in the two references listed below. These two references differ significantly in content and objectives; the first item is a research paper in which an extremely short list of axioms is stated, and the second is a book which was written to relate Birkhoff's ideas to the content and exposition of standard high school courses in geometry at the time (the book was first published in 1940).

G. D. Birkhoff, A set of postulates for plane geometry (based on scale and protractors), *Annals of Mathematics* (2) **33** (1932), pp. 329 – 345.

G. D. Birkhoff and R. Beatley, ***Basic Geometry*** (3rd Ed.). A. M. S. Chelsea Publishing, Providence, RI, 1999. ISBN: 0–821–82101–6.

More elaborate (and higher level) accounts of classical geometry based upon Birkhoff's approach appear in the textbook and online site listed below:

E. E. Moïse, ***Elementary Geometry from an Advanced Standpoint*** (3rd Ed.). Addison – Wesley, Reading, MA, 1990. ISBN: 0–201–50867–2.

http://www.math.uncc.edu/~droyster/math3181/notes/hyprgeom/hyprgeom.html

We shall call the latter ***Royster's online site***.

A brief description of the axioms

We have seen that the axioms for the real number system split naturally into three groups. One set of axioms concerns the basic properties of addition and multiplication, a second set concerns the basic properties of the linear ordering and its relationship to the arithmetic operations, and the third is the Dedekind Completeness Axiom. There is also a division of the axioms for Euclidean plane geometry into several groups. To save time and space, we shall not quote all the axioms precisely. Full statements and further information can be found in the four references cited above as well as the following sources:

E. C. Wallace and S. F. West, ***Roads to Geometry*** (3rd Ed.). Prentice – Hall, Upper Saddle River, NJ, 2003. ISBN: 0–130–41396–8.

http://math.ucr.edu/~res/math153/history03.pdf

1. Incidence axioms.

We have already discussed these.

2. Distance axioms.

We have discussed some simple properties that distance is supposed to satisfy, but the most important properties are summarized in the following strong assumption.

RULER POSTULATE. If **L** is a line, then there is a $\mathbf{1-1}$ correspondence $\mathbf{f: L \to \mathbb{R}}$ such that for all $\mathbf{x, y \in L}$ we have $\mathbf{d(x, y) = |f(x) - f(y)|}$. In other words, with respect to the given notion of distance on the plane, *every line looks like the standard real number line*.

3. Separation axiom.

In order to state this axiom correctly we must make several definitions based upon the structure developed thus far. All this is done explicitly at the online site:

http://math.ucr.edu/~res/math153/history03c.pdf

and therefore we shall only explain the key ideas. Using the Ruler Postulate one can formulate a concept of betweenness for an ordered triple of distinct collinear points. The Plane Separation Postulate is an assumption which states that for each line **L**, the points of the relative complement $\mathbb{E} - \mathbf{L}$ split into a pair of disjoint subsets, called the ***sides*** or ***(open) half – planes*** in $\mathbb{E}$ with respect to **L** and these have the expected properties involving betweenness; namely, if two points lie on the same side then every point between them also lies on that side, and if two points lie on opposite sides, then there is some point of **L** that lies between them.

4. Angular measurement axioms.

It is not possible to write these down formally without introducing numerous definitions based upon all the previous data and assumptions, so we shall simply try to summarize what happens. One needs **(1)** a simple, general criterion for constructing angles with a given measurement in a fairly arbitrary position, **(2)** an assumption that supplementary angles have measurements adding up to $\mathbf{180}$, **(3)** the usual sort of principle for concluding that the measurement of one angle is the sum of the measures of two other angles, and finally **(4)** something relating linear measures to angular measures; a standard way of doing the latter is to assume the familiar Side – Angle – Side congruence test from elementary geometry, but it is also possible to formulate everything with a simpler underlying assumption.

5. Euclidean Parallel Postuate.

This corresponds to Euclid's Fifth Postulate. For reasons related to Ockham's razor, many mathematicians starting (at least) with Proclus Diadochus (410 – 485) have preferred to take the following statement named after J. Playfair (1748 – 1819), which is logically equivalent to the original Euclid's Fifth Postulate but does not involve linear or angular measurement:

PLAYFAIR'S POSTULATE. Given a line **L** and a point **x** not on **L**, then there is a unique line **M** in the plane determined by **L** and **x** such that $\mathbf{x} \in \mathbf{M}$ but **L** and **M** do not have any points in common (since we are working in a plane, such lines are ***parallel***).

Abbreviated versions of the axioms. Partly because of Ockham's razor, and partly for reasons involving logical consistency like those stated in Section 1, it is useful to find axiomatic systems that are as economical as possible. In his 1932 paper, Birkhoff showed that one could get by with four assumptions that are simple to state but have very strong implications. There is a much different approach to making everything more concise in

http://math.ucr.edu/~res/math153/history03c.pdf

which gives a set of six relatively straightforward axioms that only involve the two "undefined concepts" of lines and distance; in this system it is possible to construct a notion of angular measurement which has all the desired properties. Of course, it is necessary to prove that such a construction is possible under the given assumptions and that the construction satisfies the required conditions. Completing these tasks takes a

significant amount of time and effort, and it relies very heavily upon numerous ideas in the following book by H. G. Forder (1889 – 1981):

> H. G. Forder, ***The foundations of Euclidean geometry*** (Reprint of the original 1927 edition). Dover Books, New York, NY, 1958.

One additional advantage of the axiom system described in the online reference is that it adapts very easily to give a set of axioms for the non – Euclidean geometry that was developed in the early 19th century by J. Bolyai (1802 – 1860) and N. Lobachevsky (1792 – 1856), and was also known to C. F. Gauss. All one needs to do is replace the final axiom.

5*. Hyperbolic Parallel Postuate.

There are two versions, but one can prove that they are logically equivalent.

STRONG VERSION. Given a line **L** and a point **x** not on **L,** then there are ***at least two*** lines **M** and **N** such that $x \in M \cap N$ but $L \cap M$ and $L \cap N$ are both empty.

WEAK VERSION. There is ***at least one pair*** **(L, x),** consisting of a line **L** and a point **x** not on the line **L,** for which there are ***at least two lines*** **M** and **N** such that $x \in M \cap N$ but $L \cap M$ and $L \cap N$ are both empty.

The weak version of the Hyperbolic Parallel Postulate is the formal negation of Playfair's Postulate; namely, the existence of unique parallels fails ***somewhere***. The strong version says it fails everywhere, and the point of logical equivalence is that ***if Playfair's Postulate fails*** **somewhere** ***then it fails*** **everywhere**. Of course, this is something that must be proved, and the material in Royster's online site gives the details.

Birkhoff's abbreviated axioms and non – Euclidean geometry. The four Birkhoff axioms in the 1932 paper cannot be simply modified to describe non – Euclidean hyperbolic geometry. The reason for this is related to the final axiom, which is the Side – Angle – Side Similarity Theorem from classical Euclidean geometry. There is no corresponding similarity theory in non – Euclidean geometry, so it is clear that one cannot get a short system of axioms for the latter by some simple changes to the Birkhoff axioms.

Relative consistency models for the axioms

The book by Moïse and the online reference by Royster show that one can obtain a complete description of the Euclidean plane or the non – Euclidean hyperbolic plane using the axioms described above. However, this does not quite imply that classical Euclidean geometry can be integrated into set theory. In order to complete the process, we need to show the following:

> ***It is possible to construct a system within set theory which satisfies all the conditions for a Euclidean plane that we have described above.***

The existence of such an example (or ***model*** *for the axioms*) will also show that the axioms satisfy an important relative consistency test; namely, the axioms for Euclidean geometry are logically consistent if the axioms for set theory are logically consistent. The online document

http://www.math.uiuc.edu/~gfrancis/M302/handouts/postulates.pdf

constructs a system of the desired type, showing that the abbreviated Birkhoff axioms are satisfied, and the document

http://math.ucr.edu/~res/math133/verifications.pdf

indicates how one can show the axioms in http://math.ucr.edu/~res/math153/history03c.pdf are also satisfied. In fact, the constructions are based upon the standard coordinate model for Euclidean geometry in which ***points*** are interpreted as ordered pairs of real numbers, ***lines*** are defined to be the sets of ordered pairs **(x, y)** satisfying the equation $\mathbf{Ax + By + C = 0}$, where *at least one* of **A, B** is nonzero, ***distance*** is defined by the usual formula in coordinate geometry, and ***angle measurement*** is defined by the standard vector formula for the cosine of an angle between to two vectors (note that the standard *Cauchy – Schwarz – Bunyakovsky inequality* in linear algebra implies this algebraically defined number lies between -1 and $+1$). Details appear on pages 5 – 7 of the online reference. Algebraic verification of the Birkhoff axioms for these definitions of lines, distance and angle measurement are summarized on pages 5 – 8 of the document cited directly above.■

There is one point in the preceding reference that deserves some thought. The inverse cosine function is of course given in terms of the cosine function, but the usual definition of the latter in trigonometry books is given geometrically. This may raise questions about whether the reasoning described in the preceding paragraph is circular. One way to answer such an objection is to define trigonometric functions, and derive the basic trigonometric identities, by some formal method that does not use Euclidean geometry explicitly (although the reasoning may/will be geometrically motivated at various points). This can be done by ***defining*** the sine and cosine to be equal to the usual power series expansions that are given in calculus and somehow proving that the functions defined by these power series have the expected properties (*e.g.*, the standard trigonometric equation $\mathbf{\sin^2 \theta + \cos^2 \theta = 1}$, or the formulas for the sine and cosine of a sum of two numbers) without using geometrical arguments. One reference for such a development of the basic trigonometric functions is pages 182 – 184 of the previously cited book by Rudin (***Principles of Mathematical Analysis***). A more elementary discussion along the same lines appears in Appendix **E** of the following book:

> P. Ryan, ***Euclidean and non-Euclidean geometry: An analytical approach.*** *Cambridge University Press,* Cambridge, U. K., and New York, NY, 1986. **ISBN:** 0–521–27635–7.

Relative consistency models for non – Euclidean geometry. One can also prove a relative consistency result for non – Euclidean geometry by constructing set – theoretic models of the corresponding axioms, but both the construction of the model and the verification of its key properties are considerably more difficult than in the Euclidean case. The models, and the verification that they satisfy the axioms, are given by results of E. Beltrami (1835 – 1900), F. Klein (1849 – 1925) and H. Poincaré (1854 – 1912) from the second half of the 19th century.

The existence of such relative consistency models is the basis for assertions that ***the parallel postulate in classical geometry cannot be proven from the other assumptions.*** If this were possible, it would contradict the existence of the models discussed in the preceding paragraph. Further discussion about the relative consistency of non – Euclidean geometry can be found on pages 255 – 258 of the following online document:

http://math.ucr.edu/~res/math133/geomnotes5b.pdf

The logical independence of the Euclidean and hyperbolic parallel postulates from the preceding assumptions is analogous to the formal status of the Axiom of Foundation, the Axiom of Choice and the Generalized Continuum Hypothesis that was discussed in the previous unit. However, there is one significant difference, for mathematicians find it convenient to view both axiom systems for geometry as equally valid, but in contexts that do not touch upon the foundations of mathematics it is generally more convenient to stick with a fixed list of axioms for set theory. Generally this is given by **ZFC** or **NBG** plus the Axiom of Choice with no assumption either way about the Generalized Continuum Hypothesis, but as we have noted there are some important exceptions, most notably the viewpoints of ***intuitionism*** and ***constructivism***. A full discussion of such matters is beyond the scope of these notes, but we shall include a list of online references for both the mainstream view of the foundations of mathematics as well as some of the alternatives:

http://sakharov.net/foundation.html

http://en.wikipedia.org/wiki/Philosophy_of_mathematics

http://en.wikipedia.org/wiki/Foundations_of_mathematics

http://www.rbjones.com/rbjpub/logic/

http://www.math.psu.edu/simpson/hierarchy.html

http://plato.stanford.edu/entries/hilbert-program/

http://en.wikipedia.org/wiki/David_Hilbert#Formalism

http://plato.stanford.edu/entries/logic-intuitionistic/

http://www.math.fau.edu/Richman/HTML/CONSTRUC.HTM

http://en.wikipedia.org/wiki/Constructivism_(mathematics)

http://plato.stanford.edu/entries/mathematics-constructive/

http://www.rbjones.com/rbjpub/philos/maths/faq025.htm

http://www.rbjones.com/rbjpub/philos/maths/faq027.htm

http://www.rbjones.com/rbjpub/philos/maths/faq004.htm

Additional remarks on alternate formulations for the foundations of mathematics (using functions rather than sets as the main building blocks) were made at the beginning of Section **IV.3.**